ESET NOD32 Antivirus 3.0

Integrierte Komponenten:
ESET NOD32 Antivirus
ESET NOD32 Antispyware

Benutzerhandbuch

we protect your digital worlds

inhalt

1. ESET NOD32 Antivirus 3.0 4
1.1 Neuerungen 4
1.2 Systemanforderungen 4

2. Installation 5
2.1 Standardinstallation 5
2.2 Benutzerdefinierte Installation 6
2.3 Vorhandene Einstellungen verwenden 7
2.4 Benutzernamen und Passwort eingeben 7
2.5 Manuelles -Prüfen des Computers 8

3. Erste Schritte 9
3.1 Übersicht zur Benutzeroberfläche – Modi 9
3.1.1 Prüfen der Funktionsfähigkeit des Systems 9
3.1.2 Vorgehensweise bei fehlerhafter Ausführung des Programms 10
3.2 Einstellungen für Updates 10
3.3 Einstellungen für den Proxyserver 10
3.4 Einstellungen schützen 11

4. ESET NOD32 Antivirus verwenden 12
4.1 Viren- und Spyware-Schutz 12
4.1.1 Echtzeit-Dateischutz 12
4.1.1.1 Prüfeinstellungen 12
4.1.1.1.1 Datenträger prüfen 12
4.1.1.1.2 Prüfen bei Ereignis- 12
4.1.1.1.3 Neu erstellte Dateien prüfen 12
4.1.1.1.4 Erweiterte Einstellungen 12
4.1.1.2 Entfernungsstufen 12
4.1.1.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden? 13
4.1.1.4 Echtzeit-Dateischutz prüfen 13
4.1.1.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz 13
4.1.2 E-Mail-Schutz 13
4.1.2.1 POP3-Prüfung 13
4.1.2.1.1 Kompatibilität 14
4.1.2.2 Integration mit Microsoft Outlook, Outlook Express und Windows Mail 14
4.1.2.2.1 E-Mail-Nachrichtentexten Prüfhinweise hinzufügen . 14
4.1.2.3 Eingedrungene Schadsoftware entfernen 15
4.1.3 Web-Schutz 15
4.1.3.1 HTTP 15
4.1.3.1.1 Blockierte/ausgeschlossene Adressen 15
4.1.3.1.2 Webbrowser 15
4.1.4 Computer prüfen 16
4.1.4.1 Prüfmethode 16
4.1.4.1.1 Standardprüfung 16
4.1.4.1.2 Prüfen mit speziellen Einstellungen 16
4.1.4.2 Zu prüfende Objekte 17
4.1.4.3 Prüfprofile 17
4.1.5 Einstellungen für ThreatSense 17
4.1.5.1 Einstellungen für zu prüfende Objekte 18
4.1.5.2 Optionen 18
4.1.5.3 Schadcode entfernen 18
4.1.5.4 Dateierweiterungen 19
4.1.6 Eingedrungene Schadsoftware wurde erkannt 19
4.2 Programm aktualisieren 20
4.2.1 Einstellungen für Updates 20
4.2.1.1 Update-Profile 20
4.2.1.2 Erweiterte Einstellungen für Updates 21
4.2.1.2.1 Update-Modus 21
4.2.1.2.2 Proxyserver 21
4.2.1.2.3 LAN-Verbindungen 22
4.2.1.2.4 Erstellen von Update-Kopien – Update-Mirror 22
4.2.1.2.4.1 Aktualisieren über Update-Mirror 23
4.2.1.2.4.2 Fehlerbehebung bei Updates über Update-Mirror .. 23
4.2.2 So erstellen Sie Update-Tasks 24

ESET NOD32 Antivirus 3.0

Copyright © 2007 ESET, spol. s r. o.

ESET NOD32 Antivirus wurde von ESET, spol. s r.o. entwickelt.
Weitere Informationen finden Sie unter www.eset.com.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Genehmigung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, die beschriebene Anwendungssoftware ohne vorherige Ankündigung zu ändern.

Weltweiter Kundendienst: www.eset.eu/support

REV.20080418-001

4.3 Taskplaner 24
4.3.1 Verwendung von Tasks 24
4.3.2 Erstellen von Tasks 24
4.4 Quarantäne 25
4.4.1 Quarantäne für Dateien 25
4.4.2 Wiederherstellen aus der Quarantäne 25
4.4.3 Senden von Dateien in Quarantäne 25
4.5 Log-Dateien 25
4.5.1 Log-Wartung 26
4.6 Benutzeroberfläche 26
4.6.1 Warnungen und Hinweise 27
4.7 ThreatSense.Net 27
4.7.1 Verdächtige Dateien 28
4.7.2 Statistik 28
4.7.3 Senden 29
4.8 Remoteverwaltung 29
4.9 Lizenz 29
5.1 Einstellungen für den Proxyserver 31
5.2 Einstellungen exportieren/importieren 31
5.2.1 Einstellungen exportieren 31
5.2.2 Einstellungen importieren 32
5.3 Kommandozeile 32

6. Glossar 33

6.1 Schadsoftwaretypen 33
6.1.1 Viren 33
6.1.2 Würmer 33
6.1.3 Trojaner 33
6.1.4 Rootkits 33
6.1.5 Adware 34
6.1.6 Spyware 34
6.1.7 Potenziell unsichere Anwendungen 34
6.1.8 Potenziell unerwünschte Anwendungen 34

1. ESET NOD32 Antivirus 3.0

ESET NOD32 Antivirus 3.0 ist der Nachfolger des preisgekrönten Produkts ESET NOD32 Antivirus 2.*. Es nutzt die Geschwindigkeit und Präzision von ESET NOD32 Antivirus, die durch Verwendung der neuesten Version der ThreatSense® Prüf-Engine gewährleistet sind.

Die implementierten fortgeschrittenen Technologien sorgen dafür, dass Viren, Spyware, Trojaner, Würmer, Adware und Rootkits proaktiv blockiert werden, ohne das System zu verlangsamen oder Sie beim Arbeiten oder Spielen am Computer zu stören.

1.1 Neuerungen

Die langjährige Erfahrung unserer Fachleute im Bereich Entwicklung wird durch die vollkommen neuartige Architektur von ESET NOD32 Antivirus unter Beweis gestellt, durch die bei minimalen Systemanforderungen ein maximaler Schutz gewährleistet wird.

- **Viren- und Spyware-Schutz**

Dieses Modul basiert auf dem Herzstück des Prüfmechanismus von ThreatSense®, der erstmals bei dem preisgekrönten -NOD 32 Antivirus-System zum Einsatz kam. Bei der Einbindung in die neue Architektur von ESET NOD32 Antivirus wurde der Kern von ThreatSense® nochmals optimiert und verbessert.

Funktion	Beschreibung
Verbessertes Entfernen von Schadcode	Das Virenschutzsystem ist in der Lage, einen Großteil der erkannten eingedrungenen Schadsoftware selbstständig zu entfernen und zu löschen, ohne dass ein Eingreifen des Benutzers nötig wäre.
Modus für Hintergrundprüfungen	Die Überprüfung des Computers kann im Hintergrund gestartet werden, ohne dass dessen Leistungsvermögen dadurch beeinträchtigt wird.
Kleinere Update-Dateien	Dank grundlegender Optimierungsprozesse sind die Update-Dateien kleiner als die für die Version 2.7 verwendeten. Auch der Schutz von Update-Dateien vor Beschädigungen ist verbessert worden.
Schutz beliebter E-Mail-Programme	Von nun an ist es möglich, eingehende E-Mails nicht nur in MS Outlook, sondern auch in Outlook Express und Windows Mail zu prüfen.
Eine Vielzahl anderer kleiner Verbesserungen	– Der direkte Zugang zu Dateisystemen sorgt für eine höhere Geschwindigkeit und einen größeren Datendurchsatz. – Bei infizierten Dateien wird der Zugriff blockiert. – Optimierung für das Windows-Sicherheitscenter, einschließlich Vista.

1.2 Systemanforderungen

Für einen reibungslosen Betrieb von ESET NOD32 Antivirus sollte Ihr System die folgenden Hardware- und Softwareanforderungen erfüllen:

ESET NOD32 Antivirus:

Windows 2000, XP	400 MHz 32-Bit/64-Bit (x86/x64) 128 MB RAM Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)
Windows Vista	1 GHz 32-Bit/64-Bit (x86/x64) 512 MB RAM Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)

ESET NOD32 Antivirus Business Edition:

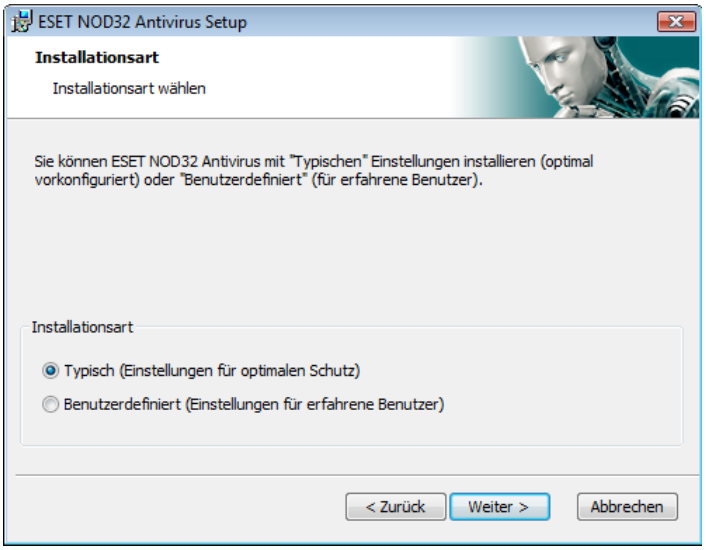
Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32-Bit/64-Bit (x86/x64) 128 MB RAM Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)
Windows Vista, Windows Server 2008	1 GHz 32-Bit/64-Bit (x86/x64) 512 MB RAM Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)

2. Installation

Nach dem Kauf des Programms können Sie das ESET NOD32 Antivirus-Installationsprogramm von der ESET-Website als MSI-Paket herunterladen. Starten Sie das Installationsprogramm. Der Installationsassistent unterstützt Sie bei der Installation. Es stehen zwei Installationsmodi zur Verfügung, die unterschiedlich viele Einstellungsmöglichkeiten bieten:

1. Standardinstallation

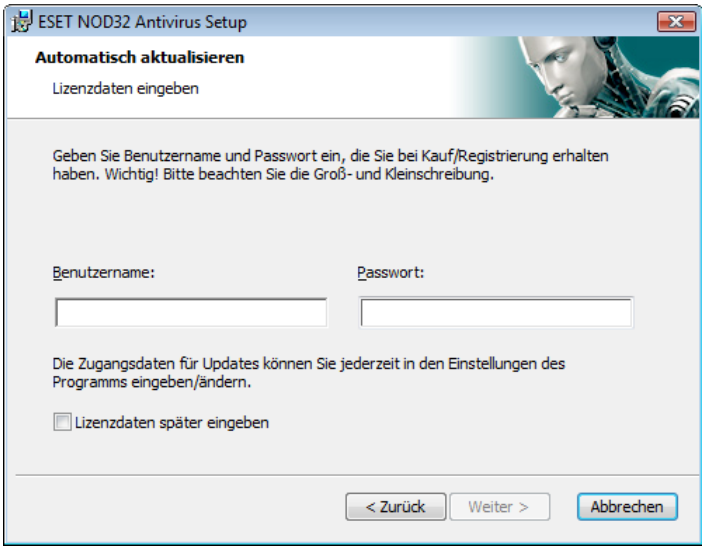
2. Benutzerdefinierte Installation


ESET NOD32 Antivirus Setup
Installationsart
Installationsart wählen
Sie können ESET NOD32 Antivirus mit "Typischen" Einstellungen installieren (optimal vorkonfiguriert) oder "Benutzerdefiniert" (für erfahrene Benutzer).
Installationsart
Typisch (Einstellungen für optimalen Schutz)
Benutzerdefiniert (Einstellungen für erfahrene Benutzer)
< Zurück
Weiter >
Abbrechen

2.1 Standardinstallation

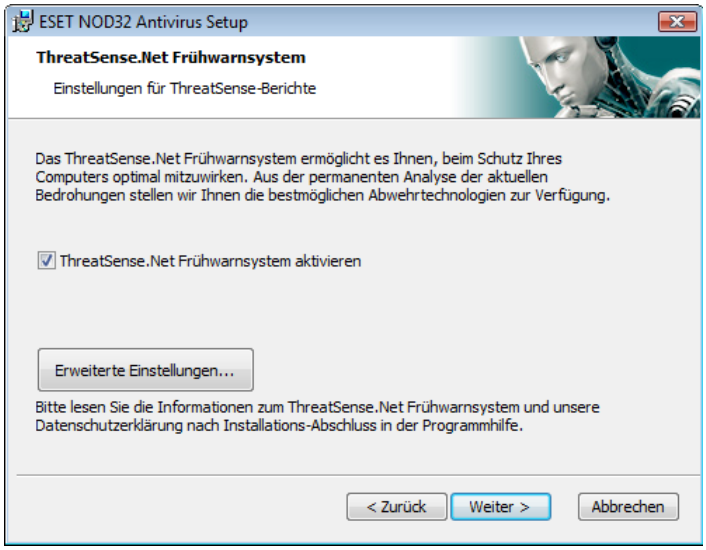
Die Standardinstallation wird Benutzern empfohlen, die ESET NOD32 Antivirus mit den Standardeinstellungen installieren möchten. Die Standardeinstellungen des Programms bieten maximalen Schutz. Für weniger erfahrene Benutzer, die detaillierte Einstellungen nicht selbst vornehmen möchten, ist daher die Standardinstallation die richtige Wahl.

Der erste (sehr wichtige) Schritt ist die Eingabe des Benutzernamens und des Passworts für die automatische Aktualisierung des Programms. Dies ist erforderlich, damit ein kontinuierlicher Schutz des Systems gewährleistet werden kann.


ESET NOD32 Antivirus Setup
Automatisch aktualisieren
Lizenzdaten eingeben
Geben Sie Benutzername und Passwort ein, die Sie bei Kauf/Registrierung erhalten haben. Wichtig! Bitte beachten Sie die Groß- und Kleinschreibung.
Benutzername:
Passwort:
Die Zugangsdaten für Updates können Sie jederzeit in den Einstellungen des Programms eingeben/ändern.
Lizenzdaten später eingeben
< Zurück
Weiter >
Abbrechen

Geben Sie in den entsprechenden Feldern Ihren **Benutzernamen** und Ihr **Passwort** ein, also die Authentifizierungsdaten, die Sie beim Kauf oder bei der Registrierung des Produkts erhalten haben. Falls Sie Ihren Benutzernamen und Ihr Passwort gerade nicht zur Hand haben, wählen Sie die Option **Zugangsdaten später eingeben**. Die Zugangsdaten können zu einem beliebigen späteren Zeitpunkt direkt vom Programm aus eingegeben werden.

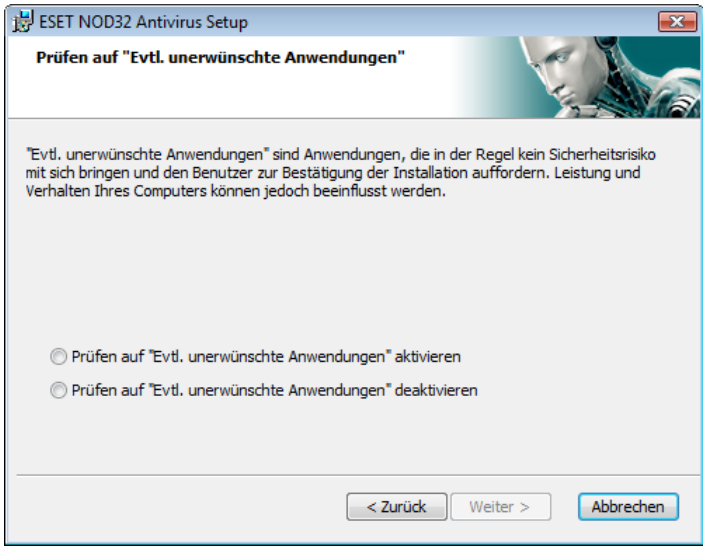
Der nächste Installationsschritt besteht in der Konfiguration des ThreatSense.Net-Frühwarnsystems. Über das ThreatSense.Net-Frühwarnsystem erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuer Schadsoftware, um dem Benutzer umfassenden Schutz zu bieten. Das Frühwarnsystem übermittelt neue Bedrohungen an ESET, wo die fraglichen Dateien analysiert, bearbeitet und zur Signaturdatenbank hinzugefügt werden.


ESET NOD32 Antivirus Setup
ThreatSense.Net Frühwarnsystem
Einstellungen für ThreatSense-Berichte
Das ThreatSense.Net Frühwarnsystem ermöglicht es Ihnen, beim Schutz Ihres Computers optimal mitzuwirken. Aus der permanenten Analyse der aktuellen Bedrohungen stellen wir Ihnen die bestmöglichen Abwehrtechnologien zur Verfügung.
ThreatSense.Net Frühwarnsystem aktivieren
Erweiterte Einstellungen...
Bitte lesen Sie die Informationen zum ThreatSense.Net Frühwarnsystem und unsere Datenschutzerklärung nach Installations-Abschluss in der Programmhilfe.
< Zurück
Weiter >
Abbrechen

Standardmäßig ist das Kontrollkästchen **ThreatSense.Net-Frühwarnsystem aktivieren** zum Aktivieren dieser Funktion aktiviert. Klicken Sie auf **Erweiterte Einstellungen**, um Einstellungen für das Einsenden verdächtiger Dateien festzulegen.

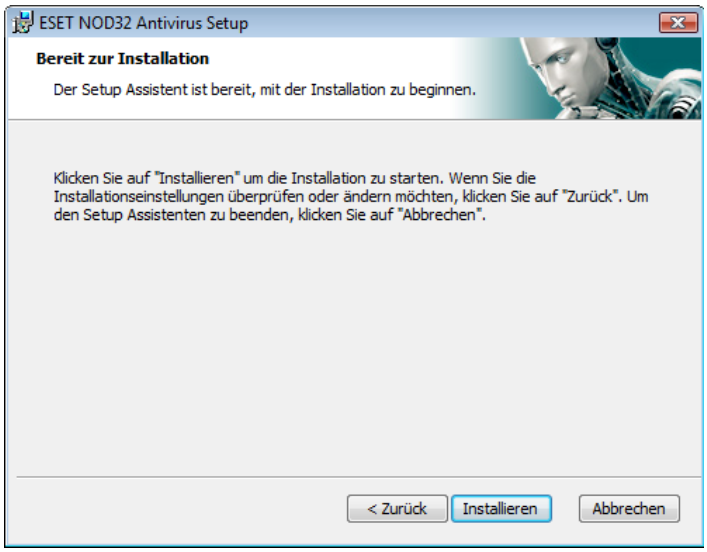
Der nächste Schritt im Installationsprozess ist die Konfiguration der Option **Prüfen auf evtl. unerwünschte Anwendungen**. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können.

Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.


ESET NOD32 Antivirus Setup
Prüfen auf "Evtl. unerwünschte Anwendungen"
"Evtl. unerwünschte Anwendungen" sind Anwendungen, die in der Regel kein Sicherheitsrisiko mit sich bringen und den Benutzer zur Bestätigung der Installation auffordern. Leistung und Verhalten Ihres Computers können jedoch beeinflusst werden.
Prüfen auf "Evtl. unerwünschte Anwendungen" aktivieren
Prüfen auf "Evtl. unerwünschte Anwendungen" deaktivieren
< Zurück
Weiter >
Abbrechen

Aktivieren Sie die Option **Prüfen auf evtl. unerwünschte Anwendungen aktivieren**, um die Prüfung dieser Art von Bedrohung durch ESET NOD32 Antivirus zuzulassen (empfohlen).

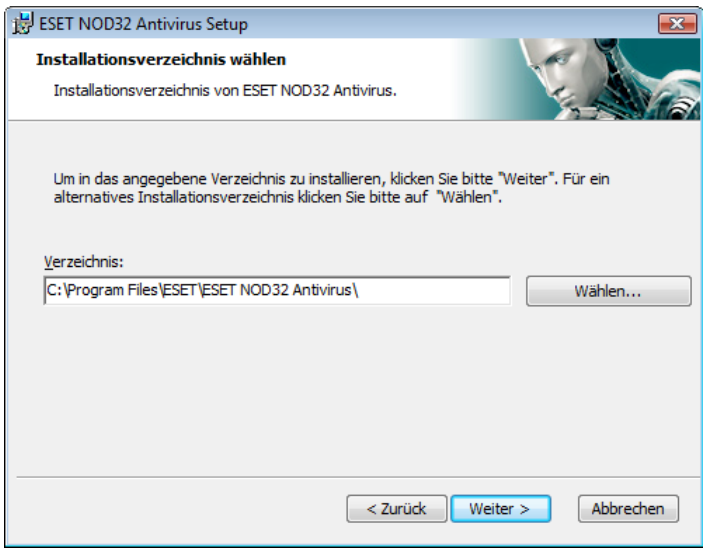
Der letzte Schritt im Standard-Installationsmodus ist die Bestätigung der Installation. Klicken Sie dazu auf die Schaltfläche **Installieren**.


ESET NOD32 Antivirus Setup
Bereit zur Installation
Der Setup Assistent ist bereit, mit der Installation zu beginnen.
Klicken Sie auf "Installieren" um die Installation zu starten. Wenn Sie die Installationseinstellungen überprüfen oder ändern möchten, klicken Sie auf "Zurück". Um den Setup Assistenten zu beenden, klicken Sie auf "Abbrechen".
< Zurück
Installieren
Abbrechen

2.2 Benutzerdefinierte Installation

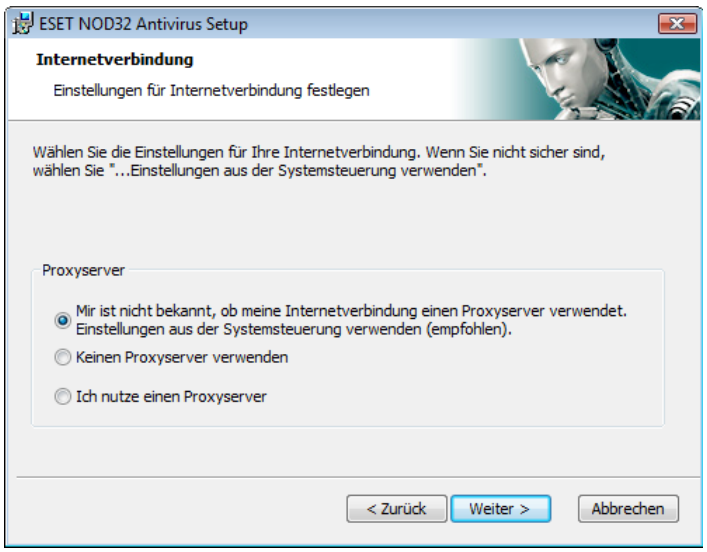
Die **benutzerdefinierte** Installation ist für erfahrene Benutzer geeignet, die während -der Installation spezielle Einstellungen vornehmen möchten.

Zunächst wird das Zielverzeichnis für die Installation ausgewählt. Standardmäßig wird das Programm im Ordner C:\Programme\ESET\ ESET Smart Security\ installiert. Klicken Sie auf **Durchsuchen...**, um einen anderen Speicherort anzugeben (nicht empfohlen).

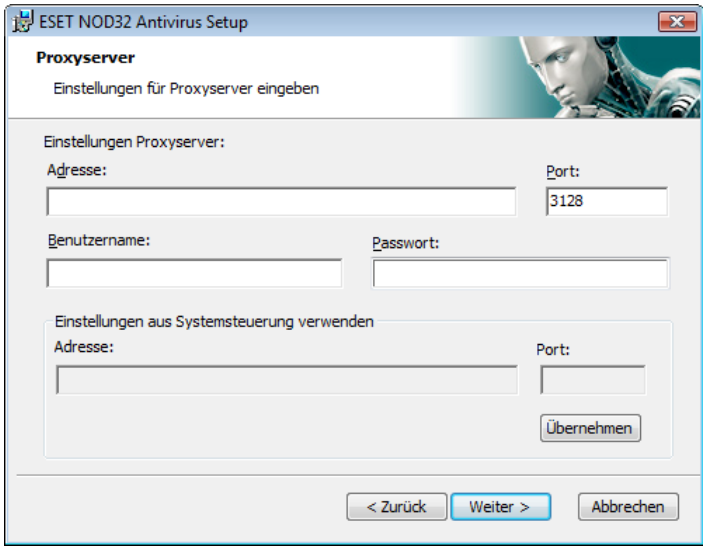

ESET NOD32 Antivirus Setup
Installationsverzeichnis wählen
Installationsverzeichnis von ESET NOD32 Antivirus.
Um in das angegebene Verzeichnis zu installieren, klicken Sie bitte "Weiter". Für ein alternatives Installationsverzeichnis klicken Sie bitte auf "Wählen".
Verzeichnis:
C:\Program Files\ESET\ESET NOD32 Antivirus\
Wählen...
< Zurück
Weiter >
Abbrechen

Im nächsten Schritt müssen Sie **Benutzernamen und Passwort eingeben**. Dieser Schritt wird wie bei der Standardinstallation (siehe Seite 5) durchgeführt.

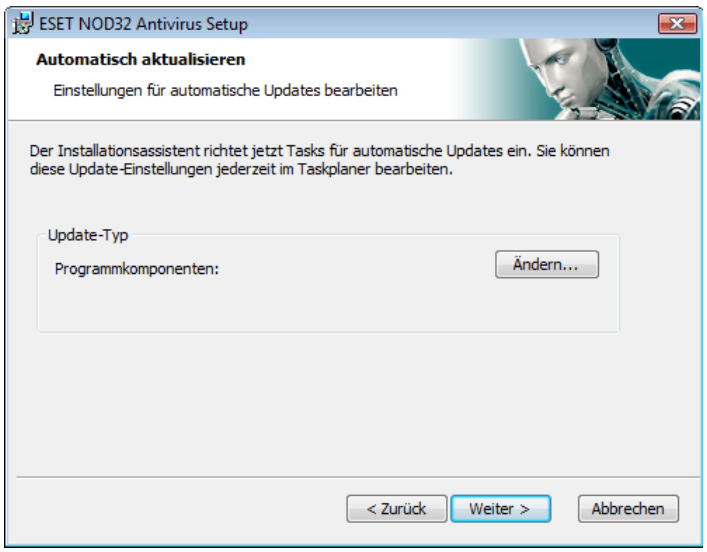
Nachdem Sie Benutzernamen und Passwort eingegeben haben, klicken Sie auf **Weiter**, um **Einstellungen für die Internetverbindung festzulegen**.


ESET NOD32 Antivirus Setup
Internetverbindung
Einstellungen für Internetverbindung festlegen
Wählen Sie die Einstellungen für Ihre Internetverbindung. Wenn Sie nicht sicher sind, wählen Sie "...Einstellungen aus der Systemsteuerung verwenden".
Proxyserver
Mir ist nicht bekannt, ob meine Internetverbindung einen Proxyserver verwendet. Einstellungen aus der Systemsteuerung verwenden (empfohlen).
Keinen Proxyserver verwenden
Ich nutze einen Proxyserver
< Zurück
Weiter >
Abbrechen

Wenn Sie einen Proxyserver verwenden, muss dieser richtig konfiguriert sein, damit die Virensignaturen ordnungsgemäß aktualisiert werden können. Falls Sie nicht wissen, ob Sie einen Proxyserver für Internetverbindungen verwenden, wählen Sie die Standardeinstellung **Mir ist nicht bekannt, ob meine Internetverbindung einen Proxyserver verwendet. Internet Explorer-Einstellungen verwenden**, und klicken Sie auf **Weiter**. Falls Sie keinen Proxyserver verwenden, aktivieren Sie die entsprechende Option.

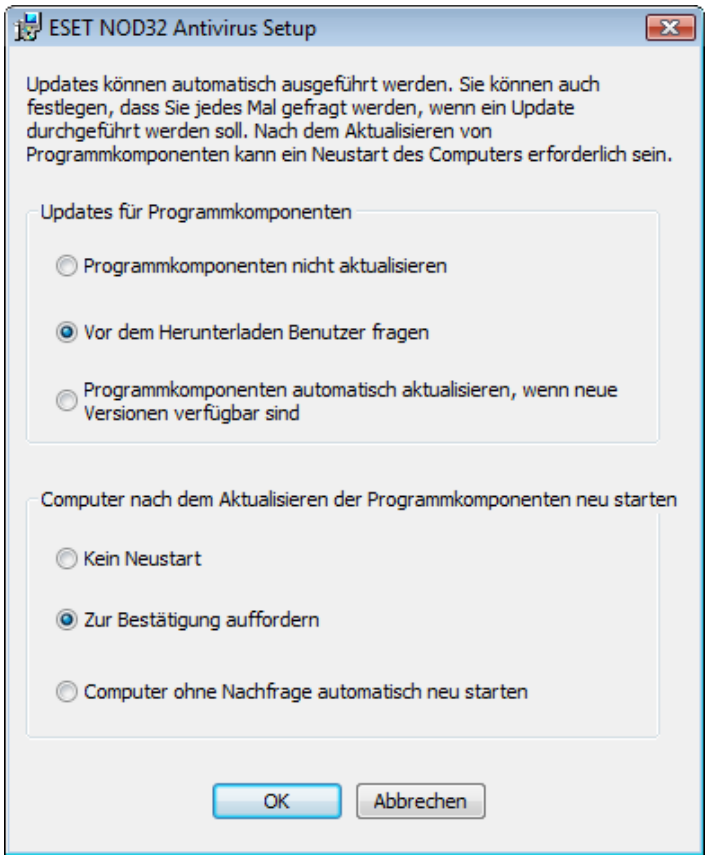


Um die Einstellungen für den Proxyserver vorzunehmen, wählen Sie **Ich nutze einen Proxyserver**, und klicken Sie auf **Weiter**. Geben Sie unter **Adresse *die IP-Adresse oder URL des Proxyservers ein.*** Unter **Port** können Sie den Port angeben, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie den gültigen Benutzernamen und das Passwort ein. Die Einstellungen für den Proxyserver können auch aus dem Internet Explorer kopiert werden, falls gewünscht. Klicken Sie dazu auf **Übernehmen**, und bestätigen Sie die Auswahl.


ESET NOD32 Antivirus Setup
Automatisch aktualisieren
Einstellungen für automatische Updates bearbeiten
Der Installationsassistent richtet jetzt Tasks für automatische Updates ein. Sie können diese Update-Einstellungen jederzeit im Taskplaner bearbeiten.
Update-Typ
Programmkomponenten:
Ändern...
< Zurück
Weiter >
Abbrechen

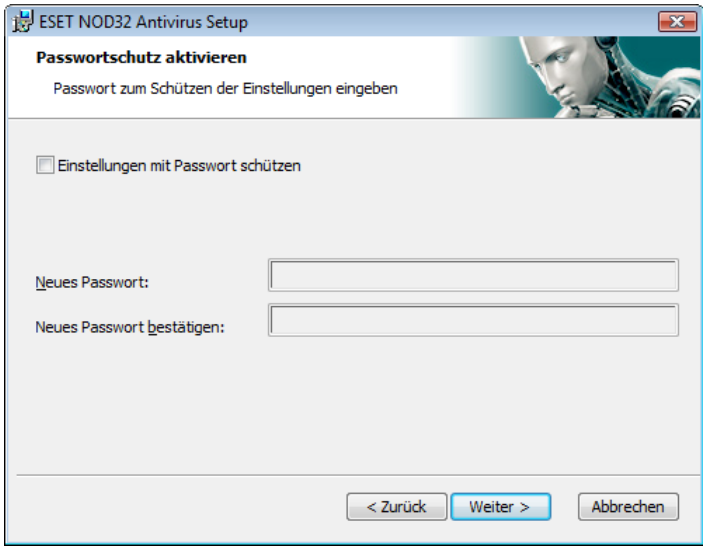
Klicken Sie auf **Weiter**, um mit dem Fenster **Einstellungen für automatische Updates bearbeiten** fortzufahren. In diesem Schritt können Sie festlegen, wie automatische Aktualisierungen von Programmkomponenten auf Ihrem System gehandhabt werden. Klicken Sie auf **Ändern...**, um erweiterte Einstellungen vorzunehmen.

Wenn Sie nicht möchten, dass Programmkomponenten aktualisiert werden, wählen Sie **Programmkomponenten nicht aktualisieren**. Wenn Sie die Option **Benutzer fragen** auswählen, wird ein Bestätigungsfenster für das Herunterladen von Programmkomponenten angezeigt. Um Programmkomponenten automatisch aktualisieren zu lassen, wählen Sie **Programmkomponenten automatisch aktualisieren, wenn neue Versionen verfügbar sind**.


ESET NOD32 Antivirus Setup
Updates können automatisch ausgeführt werden. Sie können auch festlegen, dass Sie jedes Mal gefragt werden, wenn ein Update durchgeführt werden soll. Nach dem Aktualisieren von Programmkomponenten kann ein Neustart des Computers erforderlich sein.
Updates für Programmkomponenten
Programmkomponenten nicht aktualisieren
Vor dem Herunterladen Benutzer fragen
Programmkomponenten automatisch aktualisieren, wenn neue Versionen verfügbar sind
Computer nach dem Aktualisieren der Programmkomponenten neu starten
Kein Neustart
Zur Bestätigung auffordern
Computer ohne Nachfrage automatisch neu starten
OK
Abbrechen

HINWEIS: Nach der Aktualisierung von Programmkomponenten muss der Computer üblicherweise neu gestartet werden. Dabei wird folgende Einstellung empfohlen: **Computer automatisch neu starten, ohne Nachfrage**.

Der nächste Schritt im Installationsprozess ist die Eingabe eines Passworts zum Schutz der Programmparameter. Wählen Sie ein Passwort zum Schutz des Programms. Geben Sie das Passwort zur Bestätigung erneut ein.



Die Schritte **Konfiguration des ThreatSense.Net-Frühwarnsystems** und **Prüfen auf eventuell unerwünschte Anwendungen** werden wie bei der Standardinstallation ausgeführt (siehe Seite 5).

Im Anschluss wird ein Fenster angezeigt, indem Sie die Installation bestätigen müssen.

2.3 Vorhandene Einstellungen verwenden

Wenn Sie ESET NOD32 Antivirus neu installieren, wird die Option **Vorhandene Einstellungen übernehmen** angezeigt. Wählen Sie diese Option, um die Einstellungen der ersten Installation für die neue zu übernehmen.

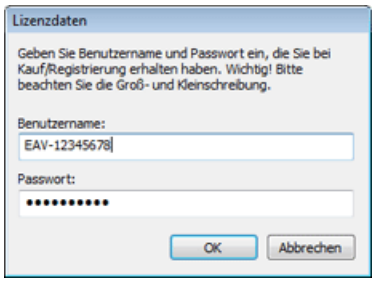
ESET NOD32 Antivirus Setup
Installationsart
Installationsart wählen
Wenn Sie die Option "Vorhandene Einstellungen übernehmen" aktivieren, werden diese bei der Neuinstallation beibehalten.
Deaktivieren Sie das Kontrollkästchen, wenn Sie die Einstellungen ändern möchten. Wählen Sie anschließend einen Installationsmodus.
Vorhandene Einstellungen übernehmen
Installationsart
Typisch (Einstellungen für optimalen Schutz)
Benutzerdefiniert (Einstellungen für erfahrene Benutzer)
< Zurück
Weiter >
Abbrechen

2.4 Benutzernamen und Passwort eingeben

Damit alle Funktionen optimal genutzt werden können, sollte das Programm automatisch aktualisiert werden. Dies ist nur möglich, wenn Benutzernamen und Passwort in den Einstellungen für Updates eingegeben wurden.

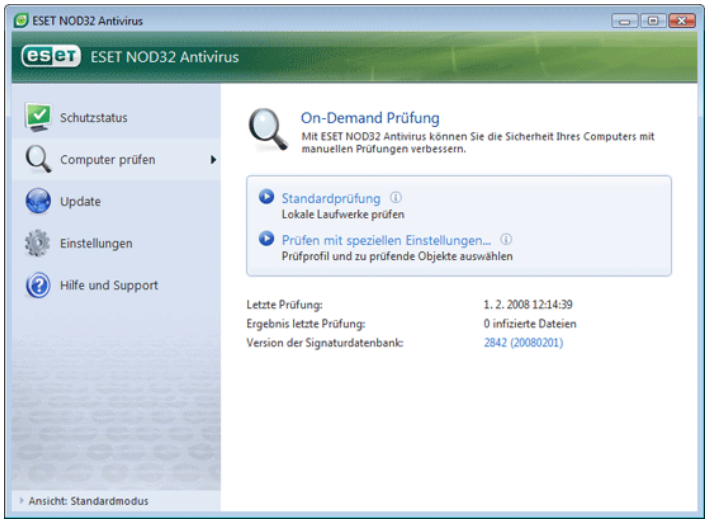
Falls Sie Ihren Benutzernamen und das Passwort während des Installationsvorgangs nicht eingegeben haben, können Sie diese Daten wie folgt eintragen: Klicken Sie im Hauptprogrammfenster auf **Update** und dann auf **Benutzernamen und Passwort festlegen...**.

Geben Sie die Daten, die Sie mit Ihrer Produktlizenz erhalten haben, im Fenster **Lizenzdaten** ein.



2.5 Manuelles -Prüfen des Computers

Nach der Installation von ESET NOD32 Antivirus sollte geprüft werden, ob auf dem Computer schädlicher Code vorhanden ist. Um eine schnelle Überprüfung auszuführen, wählen Sie im Hauptmenü **Computer prüfen**. Klicken Sie anschließend im Hauptprogrammfenster auf **Standardprüfung**. Weitere Informationen zu dieser Funktion finden Sie im Kapitel „Prüfen des Computers".



3. Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht über ESET NOD32 Antivirus und die Grundeinstellungen des Programms.

3.1 Übersicht zur Benutzeroberfläche – Modi

Das Hauptfenster von ESET NOD32 Antivirus ist in zwei Abschnitte unterteilt. In der schmaleren Spalte auf der linken Seite können Sie auf das -benutzerfreundliche Hauptmenü zugreifen. Das Hauptprogrammfenster auf der rechten Seite dient vor allem zur Anzeige von Informationen zu der im Hauptmenü ausgewählten Option.

Im Folgenden werden die Schaltflächen des Hauptmenüs beschrieben:

Schutzstatus – In -benutzerfreundlicher Form werden Informationen zum Schutzstatus von ESET Smart Security angezeigt. Wenn der erweiterte Modus aktiviert ist, wird der Status aller Schutzmodule angezeigt. Klicken sie auf ein Modul, um dessen aktuellen Status anzuzeigen.

Prüfen des Computers – In diesem Abschnitt kann bei -Bedarf eine Prüfung des Computers gestartet werden.

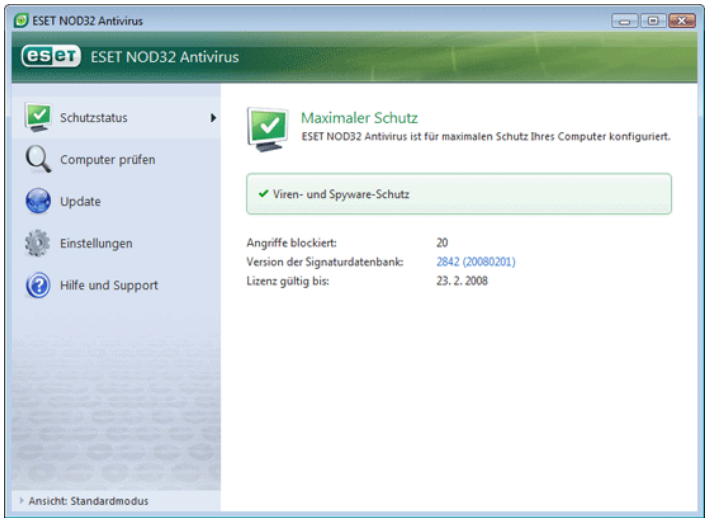
Update – Wählen Sie diese Option, um das Update-Modul aufzurufen, mit dem Updates für Programme verwaltet werden können.

Einstellungen – Wählen Sie diese Option, um die Sicherheitsstufe Ihres Computers anzupassen. Im erweiterten Modus werden zusätzlich die Untermenüs für Viren- und Spyware-Schutz angezeigt.

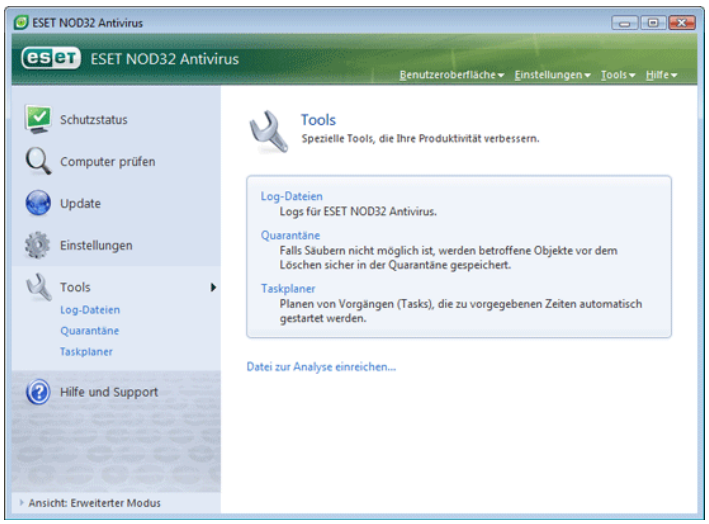
Extras – Diese Option steht nur im erweiterten Modus zur Verfügung. Sie erlaubt den Zugriff auf Log-Dateien, Quarantäne und den Taskplaner.

Hilfe und Support – Wählen Sie diese Option, um auf die Datenbank und die Website von ESET zuzugreifen oder den Kundendienst anzufordern.

Innerhalb der Benutzeroberfläche von ESET NOD32 Antivirus kann der Benutzer zwischen dem Standardmodus und dem erweiterten Modus wechseln. Um zwischen diesen Einstellungen umzuschalten, nutzen Sie den Link **Anzeige** unten links im Hauptbildschirm von ESET NOD32 Antivirus. Klicken Sie auf diese Schaltfläche, um den gewünschten Anzeigemodus auszuwählen.



Im Standardmodus können Sie auf Funktionen zugreifen, die für allgemeine Vorgänge benötigt werden. Die erweiterten Einstellungen werden nicht angezeigt.

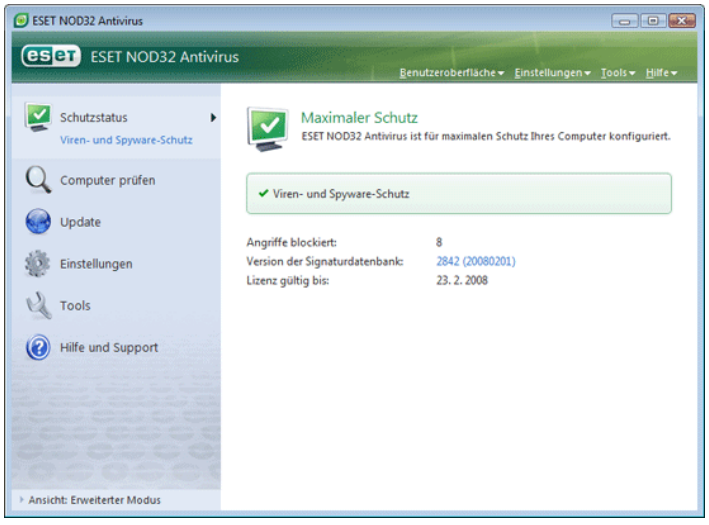


Beim Wechsel in den erweiterten Modus wird dem Hauptmenü die Option **Extras** hinzugefügt. Über die Option „Extras" können Sie auf Taskplaner und Quarantäne zugreifen und Log-Dateien von ESET NOD32 Antivirus anzeigen.

HINWEIS: Die weiteren Anweisungen in diesem Handbuch beziehen sich auf den erweiterten Modus.

3.1.1 Prüfen der Funktionsfähigkeit des Systems

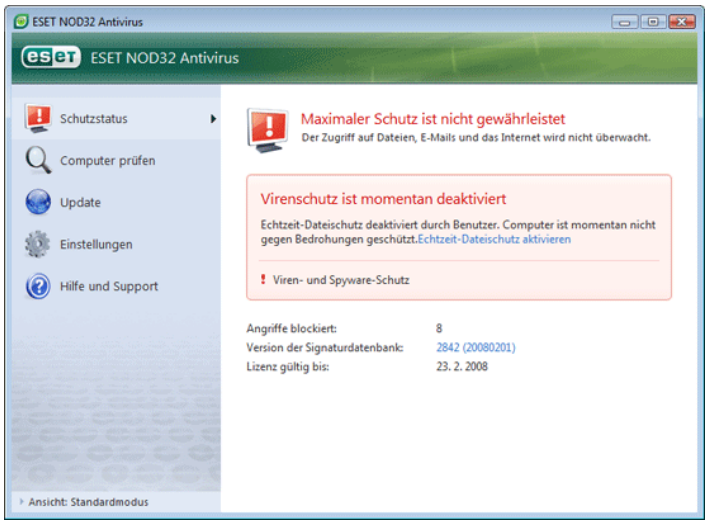
Zum Anzeigen des **Schutzstatus** klicken Sie oben im Hauptmenü auf die entsprechende Option. Das Untermenü **Viren- und Spyware-Schutz** wird direkt darunter angezeigt, eine Darstellung des aktuellen Betriebszustands von ESET NOD32 Antivirus wird im Hauptprogrammfenster angezeigt. Klicken Sie auf „Viren- und Spyware-Schutz", um im Hauptprogrammfenster den Status der einzelnen Schutzmodule anzuzeigen.



Wenn die aktivierten Module ordnungsgemäß arbeiten, sind sie grün markiert. Andernfalls wird ein rotes oder orangefarbenes Symbol angezeigt. Weitere Informationen zu dem Modul erhalten Sie im oberen Teil des Fensters. Unter anderem finden Sie dort einen Vorschlag zur Behebung des Problems. Um den Status einzelner Module zu ändern, klicken Sie im Hauptmenü auf **Einstellungen** und wählen das gewünschte Modul aus.

3.1.2 Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn ESET NOD32 Antivirus ein Problem bei einem der Schutzmodule entdeckt, wird dies im Fenster **Schutzstatus** gemeldet. Hier finden Sie auch eine mögliche Lösung für das Problem.

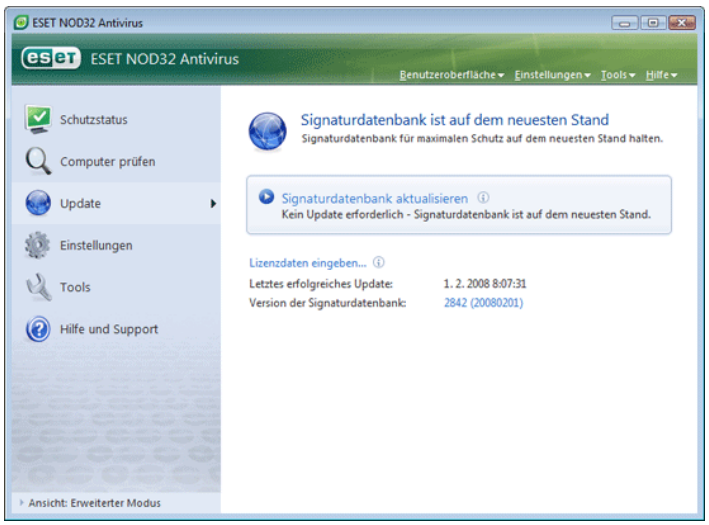

ESET NOD32 Antivirus
ESET NOD32 Antivirus
Schutzstatus
Computer prüfen
Update
Einstellungen
Hilfe und Support
Maximaler Schutz ist nicht gewährleistet
Der Zugriff auf Dateien, E-Mails und das Internet wird nicht überwacht.
Virenschutz ist momentan deaktiviert
Echtzeit-Dateischutz deaktiviert durch Benutzer. Computer ist momentan nicht gegen Bedrohungen geschützt.Echtzeit-Dateischutz aktivieren
Viren- und Spyware-Schutz
Angriffe blockiert: 8
Version der Signaturdatenbank: 2842 (20080201)
Lizenz gültig bis: 23. 2. 2008
Ansicht: Standardmodus

Wenn sich ein Problem nicht anhand der Liste bekannter Probleme und Lösungen beheben lässt, klicken Sie auf **Hilfe und Support**, um die Hilfedateien aufzurufen oder in der Datenbank zu suchen. Wenn Sie auch hier keine Lösung finden, können Sie eine Kundendienstanfrage an den ESET-Kundendienst senden. Auf Grundlage dieser Rückmeldungen können unsere Spezialisten Ihre Fragen schnell beantworten und Sie effektiv beraten.

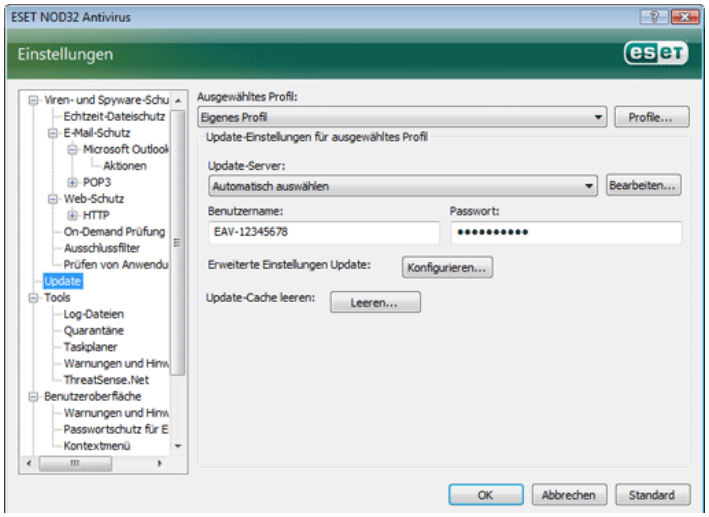
3.2 Einstellungen für Updates

Updates der Signaturdatenbank und Updates von Programmkomponenten sind ein wichtiger Bestandteil der Maßnahmen für einen möglichst umfassenden Schutz vor schädlichem Code. Seien Sie deshalb bei Konfiguration und Ausführung besonders sorgfältig. Wählen Sie im Hauptmenü die Option **Update**, und klicken Sie dann im Hauptprogrammfenster auf **Update der Signaturdatenbank**, um direkt zu überprüfen, ob ein Datenbank-Update verfügbar ist. **Benutzernamen und Passwort festlegen...** öffnet ein Dialogfeld, in dem der beim Kauf erhaltene Benutzername und das Passwort eingegeben werden.

Wenn Benutzername und Passwort bei der Installation von ESET NOD32 Antivirus eingegeben wurden, werden Sie hier nicht zu einer Eingabe aufgefordert.

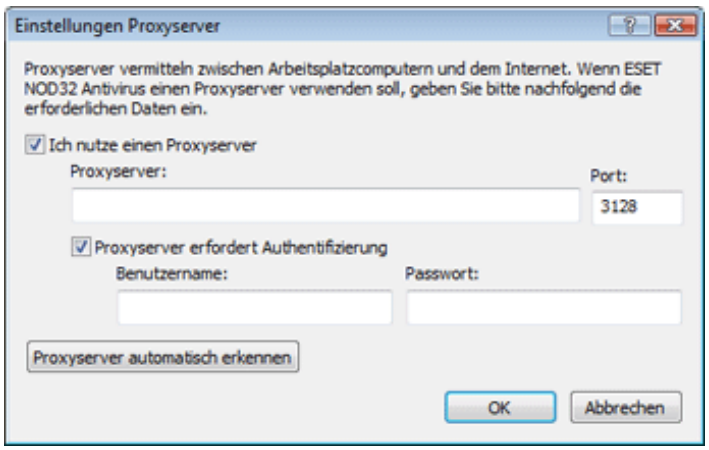


Das (durch Drücken der Taste F5 aufrufbare) Fenster **Erweiterte Einstellungen** enthält weitere Optionen für Updates. Im Dropdown-Menü **Update-Server:** sollte die Option **Automatisch auswählen** ausgewählt sein. Zum Konfigurieren erweiterter Update-Optionen wie Update-Modus, Proxyserverzugriff, Zugriff auf Updates auf einem lokalen Server und Erstellen von Signaturkopien (ESET NOD32 Antivirus Business Edition) klicken Sie auf **Einstellungen...**.



3.3 Einstellungen für den Proxyserver

Wenn Sie einen Proxyserver nutzen, um die Internetverbindung eines Systems zu vermitteln, auf dem ESET Smart Security verwendet wird, so muss dies in den erweiterten Einstellungen (F5) angegeben werden. Um das Konfigurationsfenster **Proxyserver** zu öffnen, klicken Sie unter „Erweiterte Einstellungen" auf **Allgemein > Proxyserver**. Aktivieren Sie das Kontrollkästchen **Folgenden Proxyserver verwenden**, und geben Sie die IP-Adresse und den Port des Proxyservers sowie die Authentifizierungsdaten ein.



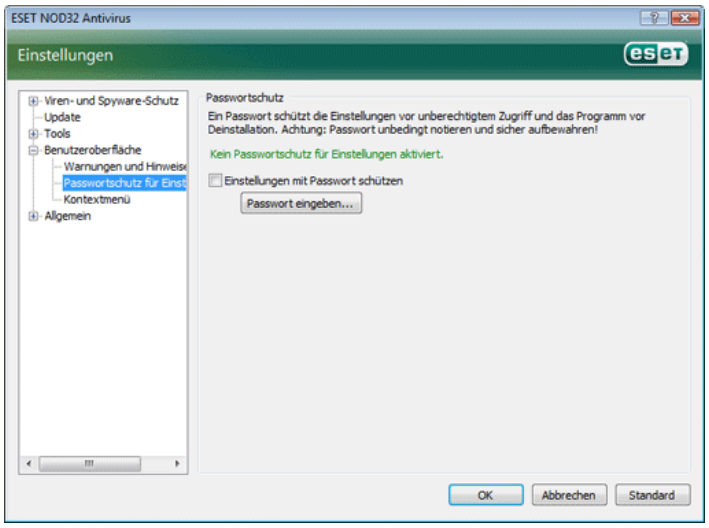
Wenn Ihnen diese Informationen nicht zur Verfügung stehen, können Sie versuchen, die Proxyservereinstellungen für ESET NOD32 Antivirus automatisch erkennen zu lassen. Dazu klicken Sie auf **Proxyserver *automatisch erkennen*** .

HINWEIS: Die Proxyserver-Optionen können für verschiedene Update-Profile abweichen. Konfigurieren Sie den Proxyserver in diesem Fall über die erweiterten Einstellungen für Updates

3.4 Einstellungen schützen

Die Einstellungen von ESET NOD32 Antivirus können im Hinblick auf die Sicherheitsrichtlinien Ihres Unternehmens von großer Wichtigkeit sein. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Um die Einstellungen mit einem Passwort zu schützen, klicken Sie im Hauptmenü auf **Einstellungen > Erweiterte Einstellungen... > Benutzeroberfläche > Einstellungen schützen,** und klicken Sie auf **Passwort eingeben...**.

Geben Sie ein Passwort ein, und bestätigen Sie es durch erneutes Eingeben. Klicken Sie anschließend auf **OK**. Dieses Passwort ist erforderlich, um künftige Änderungen an den Einstellungen von ESET NOD32 Antivirus vorzunehmen.



4. ESET NOD32 Antivirus verwenden

4.1 Viren- und Spyware-Schutz

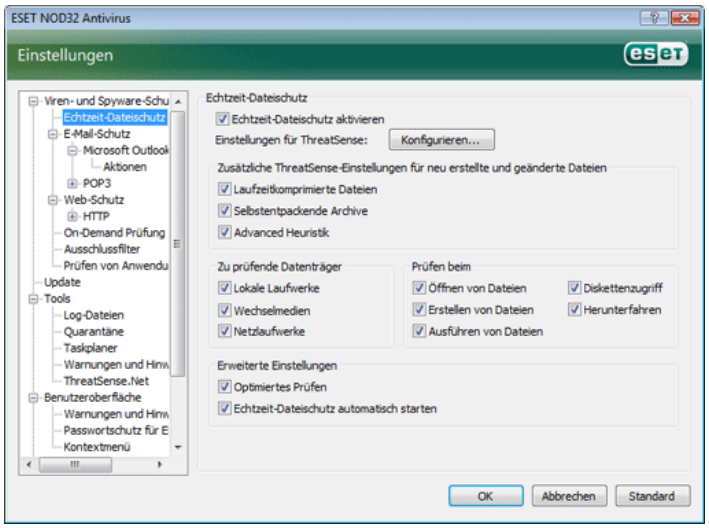
Virenschutzlösungen bieten durch Überwachung der Daten-, E-Mail- und Internet-Kommunikation Schutz vor bösartigen Systemangriffen. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es zunächst die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

4.1.1 Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz -relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf dem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird beim Systemstart gestartet.

4.1.1.1 Prüfeinstellungen

Der Echtzeit-Dateischutz prüft alle Datenträger, wobei die Prüfung von verschiedenen Ereignissen ausgelöst wird. Zum Prüfen werden ThreatSense-Erkennungsmethoden verwendet (siehe „Einstellungen für ThreatSense"). Das Prüfverhalten kann für neu erstellte Dateien und vorhandene Dateien variieren. Neu erstellte Dateien können einer noch gründlicheren Prüfung unterzogen werden.



4.1.1.1.1 Datenträger prüfen

Standardmäßig werden alle Arten von Datenträgern auf mögliche Bedrohungen geprüft.

Lokale Laufwerke – Alle Festplatten des Systems werden geprüft
Wechselmedien – Disketten, USB-Speichergeräte usw.
Netzlaufwerke – Alle verbundenen Netzlaufwerke werden geprüft

Ändern Sie diese Einstellungen nur in Ausnahmefällen, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung verlangsamt.

4.1.1.1.2 Prüfen bei Ereignis-

Standardmäßig werden alle Dateien beim Öffnen, Ausführen oder Erstellen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So verfügen Sie über maximalen Echtzeit-Dateischutz auf Ihrem Computer.

Über die Option **Diskettenzugriff** können Sie den Bootsektor einer Diskette prüfen, wenn auf das entsprechende Laufwerk zugegriffen wird. Über die Option **Herunterfahren** können Sie die Festplatten-Bootsektoren beim Herunterfahren des Computers prüfen. Auch wenn Boot-Viren heutzutage selten sind, sollten Sie diese Optionen dennoch aktivieren, da die Gefahr der Infektion durch einen Boot-Virus aus alternativen Quellen durchaus besteht.

4.1.1.1.3 Neu erstellte Dateien prüfen

Die Wahrscheinlichkeit einer Infektion ist bei neu -erstellten Dateien vergleichsweise höher als bei schon länger vorhandenen Dateien. Für die Prüfung dieser Dateien werden daher zusätzliche Parameter herangezogen. Neben gewöhnlichen Prüfmethoden auf-Signaturbasis werden erweiterte heuristische Verfahren verwendet, wodurch die Erkennungsrate deutlich steigt. Es werden nicht nur neu-erstellte Dateien, sondern auch -selbstentpackende Dateien (SFX) und laufzeitkomprimierte Dateien (intern komprimierte ausführbare Dateien) geprüft.

4.1.1.1.4 Erweiterte Einstellungen

Um die Anzahl der geprüften Objekte möglichst gering zu halten, werden Dateien, die bereits durch den Echtzeit-Dateischutz geprüft wurden, nicht erneut geprüft (außer sie wurden geändert). Dateien werden nach jedem Update der Signaturdatenbank umgehend erneut geprüft. Dieses Verhalten wird über die Option **Optimiertes Prüfen** konfiguriert. Ist diese Option deaktiviert, werden alle Dateien bei jedem Zugriff geprüft.

Der Echtzeit-Dateischutz wird standardmäßig beim Starten des Betriebssystems gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei einem Konflikt mit einer anderen Echtzeit-Prüfung) kann die Ausführung des Echtzeit-Dateischutzes abgebrochen werden. Deaktivieren Sie dazu die Option **Echtzeit-Dateischutz automatisch starten**.

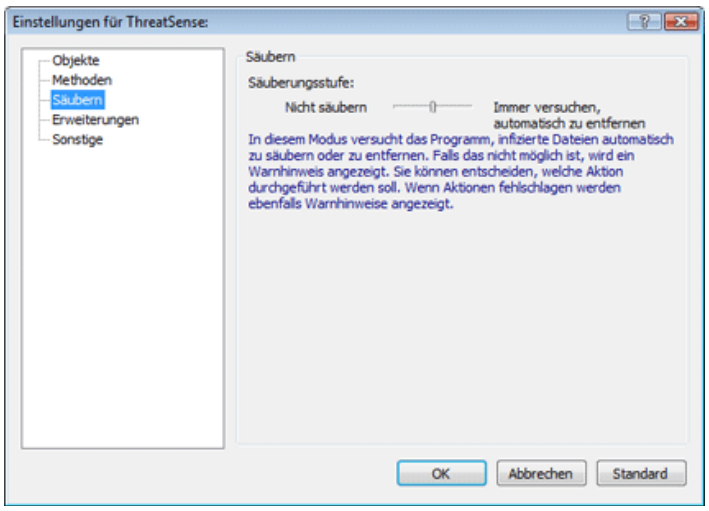
4.1.1.2 Entfernungsstufen

Der Echtzeit-Dateischutz verfügt über drei Entfernungsstufen (um darauf zuzugreifen, klicken Sie im Bereich **Echtzeit-Dateischutz** auf **Einstellungen...**, und wählen Sie dann **Schadcode entfernen**).

- Auf der ersten Entfernungsstufe wird für jede erkannte eingedrungene Schadsoftware eine Warnung angezeigt, die eine Auswahl an Optionen bereitstellt. Der Benutzer muss für jede eingedrungene Schadsoftware eine eigene Aktion auswählen. Diese Stufe eignet sich vor allem für fortgeschrittene Benutzer, die wissen, wie sie mit den verschiedenen Schadsoftwaretypen umzugehen haben.

- Auf der mittleren Stufe wird automatisch eine vordefinierte Aktion ausgewählt und ausgeführt, je nach Typ der eingedrungenen Schadsoftware. Eine Informationsnachricht am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Eine automatische Aktion wird nicht ausgeführt, wenn sich die infizierte Datei in einem Archiv befindet und dieses weitere nicht infizierte Dateien enthält. Gleiches gilt für Objekte, für die keine vordefinierte Aktion angegeben wurde.

- Die dritte Entfernungsstufe ist am „aggressivsten", der Schadcode aller infizierten Objekte wird entfernt. Da hierbei möglicherweise wichtige Dateien verloren gehen, sollten Sie auf diesen Modus nur in besonderen Fällen zurückgreifen.


Einstellungen für ThreatSense:
Objekte
Methoden
Säubern
Erweiterungen
Sonstige
Säubern
Säuberungsstufe:
Nicht säubern
Immer versuchen, automatisch zu entfernen
In diesem Modus versucht das Programm, infizierte Dateien automatisch zu säubern oder zu entfernen. Falls das nicht möglich ist, wird ein Warnhinweis angezeigt. Sie können entscheiden, welche Aktion durchgeführt werden soll. Wenn Aktionen fehlschlagen werden ebenfalls Warnhinweise angezeigt.
OK
Abbrechen
Standard

4.1.1.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Daher sollte gründlich geprüft werden, ob eine Änderung der Einstellungen wirklich notwendig ist. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu verändern. Es kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung oder der Echtzeit-Prüfung eines anderen Virenschutzprogramms vorliegt.

Bei der Installation von ESET NOD32 Antivirus werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**, die sich unten rechts im Fenster **Echtzeit-Dateischutz** befindet (**Erweiterte Einstellungen > Viren- und Spyware-Schutz > Echtzeit-Dateischutz**).

4.1.1.4 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz ordnungsgemäß funktioniert und Viren erkennt, verwenden Sie eine Testdatei von eicar.com. Bei dieser Testdatei handelt es sich um eine spezielle, harmlose Datei, die von allen Virenschutzprogrammen erkannt wird. Die Datei wurde von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen. Die Datei „eicar.com" kann unter http://www.eicar.org/download/eicar.com heruntergeladen werden.

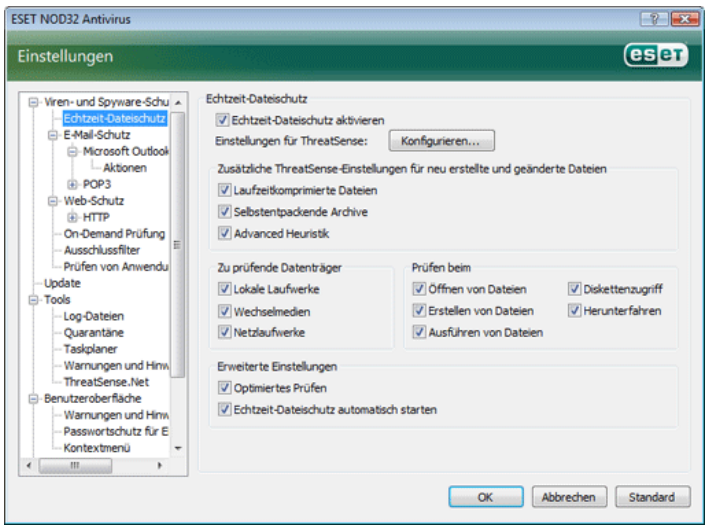
4.1.1.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

Im nächsten Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz wieder zu aktivieren, wählen Sie **Einstellungen > Viren- und Spyware-Schutz**, und klicken Sie im Bereich **Echzeit-Dateischutz** des Hauptprogrammfensters auf **Aktivieren**.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht gestartet wird, liegt das wahrscheinlich daran, dass die Option **Echtzeit-Dateischutz automatisch starten** deaktiviert ist. Um die Option zu aktivieren, wählen Sie **Erweiterte Einstellungen** (F5), und klicken Sie dort auf **Echtzeit-Dateischutz**. Vergewissern Sie sich, dass im Bereich **Erweiterte Einstellungen** im unteren Teil des Fensters das Kontrollkästchen **Echtzeit-Dateischutz automatisch starten** aktiviert ist.



Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Echtzeit-Schutzprogramme können miteinander in Konflikt geraten. Es wird empfohlen, andere Virenschutzprogramme auf dem Computer zu deinstallieren.

Echtzeit-Dateischutz startet nicht

Wenn der Echtzeit-Dateischutz beim Systemstart nicht aktiviert wird (während die Option **Echtzeit-Dateischutz automatisch starten** aktiviert ist), kann dies durch Konflikte mit anderen Programmen verursacht werden. Sollte dies der Fall sein, wenden Sie sich an einen der Experten des ESET-Kundendienstes.

4.1.2 E-Mail-Schutz

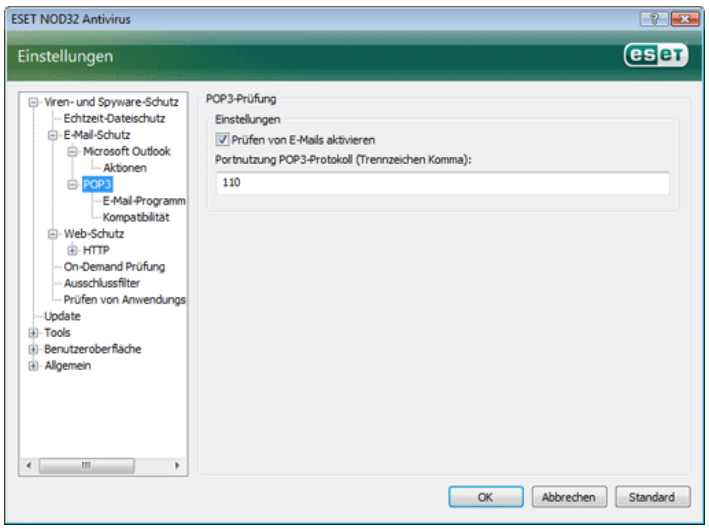
Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. Mithilfe der Plugin-Software für Microsoft Outlook stellt ESET NOD32 Antivirus Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Signaturdatenbank statt. Die Prüfung der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

4.1.2.1 POP3-Prüfung

Das POP3-Protokoll ist das am häufigsten verwendete Protokoll zum Empfangen von E-Mail-Nachrichten mit einem E-Mail-Programm. ESET NOD32 Antivirus bietet POP3-Protokoll-Schutzfunktionen unabhängig vom verwendeten E-Mail-Programm.

Das Modul, das diese Kontrollfunktion bereitstellt, wird automatisch beim Start des Betriebssystems initialisiert und ist dann im Speicher aktiv. Um das Modul einsetzen zu können, muss es aktiviert sein. Die POP3-Prüfung wird automatisch ausgeführt, und die E-Mail-Software muss nicht neu konfiguriert werden. In der Standardeinstellung wird die gesamte Kommunikation über Port 110 geprüft. Bei Bedarf können weitere Kommunikationsports hinzugefügt werden. Portnummern müssen durch ein Komma voneinander getrennt sein.

Verschlüsselte Kommunikation wird nicht geprüft.



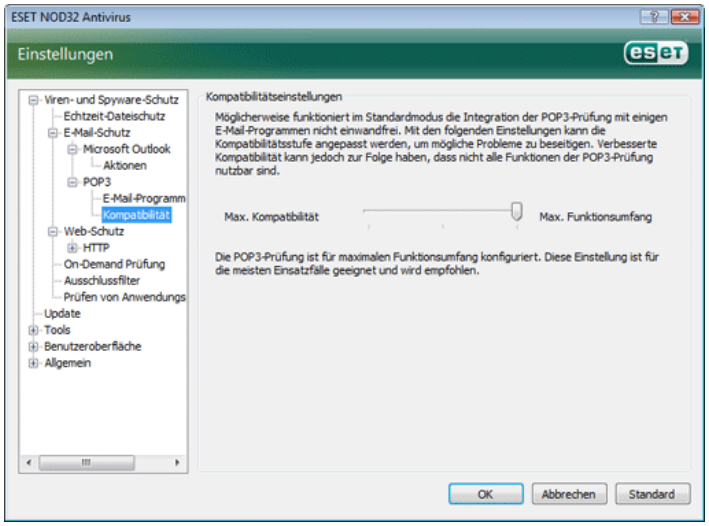
4.1.2.1.1 Kompatibilität

Bei bestimmten E-Mail-Programmen können Probleme mit der POP3-Prüfung auftreten (wenn Sie z. B. eine langsame Internetverbindung verwenden, kann es beim Prüfen zu Zeitüberschreitungen kommen). Sollte dies der Fall sein, ändern Sie die Prüfeinstellungen. Wenn Sie die Prüfmethoden lockern, kann das Entfernen von Schadcode beschleunigt werden. Um die Stufe der POP3-Prüfung anzupassen, wählen Sie **Viren- und Spyware-Schutz > E-Mail-Schutz > POP3 > Kompatibilität**.

Bei Aktivierung der Option **Maximaler Funktionsumfang** wird eingedrungener Schadcode aus infizierten Nachrichten entfernt (wenn die Optionen **Löschen** oder **Entfernen** aktiviert sind oder die Entfernungsstufen **Immer versuchen, automatisch zu entfernen** oder **Standard** aktiviert sind).

Mittlere Kompatibilität ändert die Art und Weise, wie Nachrichten empfangen werden. Nachrichten werden stückweise an das E-Mail-Programm gesendet, und nachdem der letzte Teil der Nachricht übertragen wurde, wird die Nachricht auf Schadcode geprüft. Bei dieser Prüfmethode steigt das Infektionsrisiko. Die Entfernungsstufe und die Behandlung von Prüfhinweisen (Warnhinweise, die an die Betreffzeile und den E-Mail-Nachrichtentext angehängt werden) entsprechen den Einstellungen der Option „Maximaler Funktionsumfang".

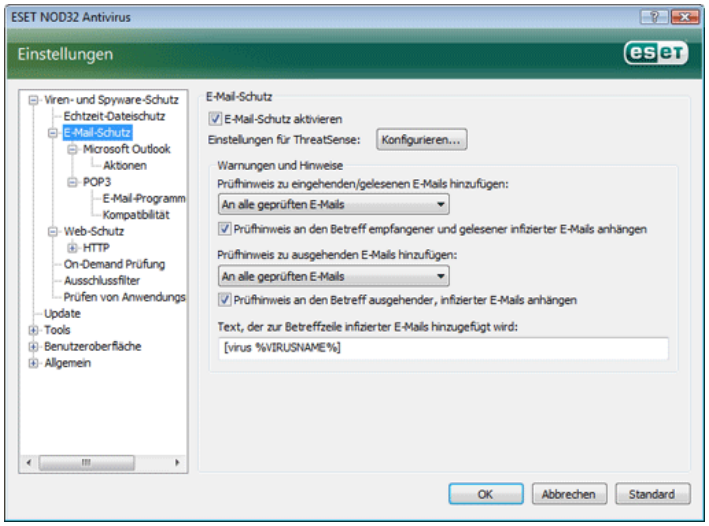
Bei der Stufe **Maximale Kompatibilität** wird der Benutzer mit Hilfe eines Alarmfensters über den Empfang einer infizierten Nachricht informiert. Es werden keine Informationen über infizierte Dateien an die Betreffzeile oder den Text eingegangener Nachrichten angehängt, und eingedrungener Schadcode wird nicht automatisch entfernt. Den Schadcode muss der Benutzer vom E-Mail-Programm aus entfernen.



4.1.2.2 Integration mit Microsoft Outlook, Outlook Express und Windows Mail

Die Integration von ESET NOD32 Antivirus mit E-Mail-Programmen verbessert den aktiven Schutz vor Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm unterstützt wird, können Sie diese Integration in ESET Smart Security aktivieren. Bei aktivierter Integration wird die Spam-Schutz-Symbolleiste von ESET NOD32 Antivirus direkt in das E-Mail-Programm eingebunden. Auf diese Weise können E-Mails effizienter geschützt werden. Die Integrationseinstellungen finden Sie unter **Einstellungen > Erweiterte Einstellungen... > Allgemein > Integration mit E-Mail-Programmen**. Über dieses Dialogfeld können Sie die Integration mit den unterstützten E-Mail-Programmen aktivieren. Aktuell werden die E-Mail-Programme Microsoft Outlook, Outlook Express and Windows Mail unterstützt.

Der E-Mail-Schutz wird gestartet, indem Sie das Kontrollkästchen **E-Mail-Schutz aktivieren** unter **Erweiterte Einstellungen (F5)** > **Viren- und Spyware-Schutz** > **E-Mail-Schutz** *aktivieren*.



4.1.2.2.1 E-Mail-Nachrichtentexten Prüfhinweise hinzufügen

An den Betreff oder den Nachrichtentext jeder E-Mail, die von ESET NOD32 Antivirus überwacht wird, kann ein Prüfhinweis angehängt werden. Diese Funktion erhöht die Glaubwürdigkeit der von einem Benutzer gesendeten Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen hilfreiche Informationen zur Verfügung, um den Bedrohungsgrad durch den Sender einzuschätzen.

Die Optionen für diese Funktion werden unter **Erweiterte Einstellungen > Viren- und Spyware-Schutz > E-Mail-Schutz** festgelegt. Das Programm kann sowohl einen **Prüfhinweis zu eingehenden E-Mails hinzufügen** als auch einen **Prüfhinweis zu ausgehenden E-Mails hinzufügen**. Für beide Optionen kann der Benutzer festlegen, ob jeder E-Mail, nur infizierten E-Mails oder gar keiner E-Mail ein Prüfhinweis angehängt werden soll.

Mit ESET NOD32 Antivirus können Sie auch dem Original-Betreff infizierter Nachrichten Prüfhinweise anhängen. Zum Aktivieren dieser Funktion verwenden Sie die Optionen **Prüfhinweis zum Betreff eingehender E-Mails hinzufügen (nur infizierte E-Mails)** und **Prüfhinweis zum Betreff ausgehender E-Mails hinzufügen (nur infizierte E-Mails)**.

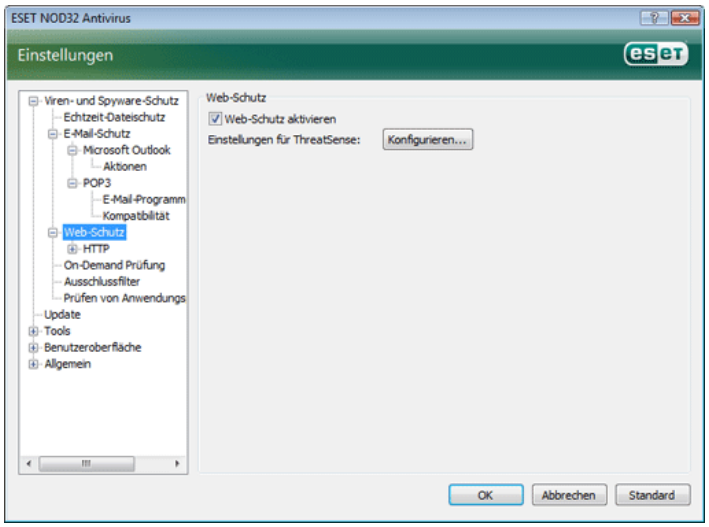
Der Inhalt der Hinweise kann im Feld „Vorlage" bearbeitet und dem Betreff der infizierten E-Mails hinzugefügt werden. Die oben genannten Änderungen dienen dazu, die Filterung infizierter E-Mails zu automatisieren, indem E-Mail-Nachrichten mit einem bestimmten Betreff in einen getrennten Ordner aussortiert werden können (falls von Ihrem E-Mail-Programm unterstützt).

4.1.2.3 Eingedrungene Schadsoftware entfernen

Bei Empfang einer infizierten E-Mail-Nachricht wird eine Warnung angezeigt. Die Warnung enthält den Namen des Absenders, die E-Mail und den Namen der eingedrungenen Schadsoftware. Im unteren Bereich des Fensters können Sie zwischen den Optionen **Säubern**, **Löschen** oder **Belassen** für das entdeckte Objekt auswählen. In fast allen Fällen sollten Sie entweder **Säubern** oder **Löschen** wählen. Um die infizierte Datei in Ausnahmesituationen zu empfangen, wählen Sie **Belassen**. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird ein Informationsfenster ohne Auswahloptionen für das infizierte Objekt angezeigt.

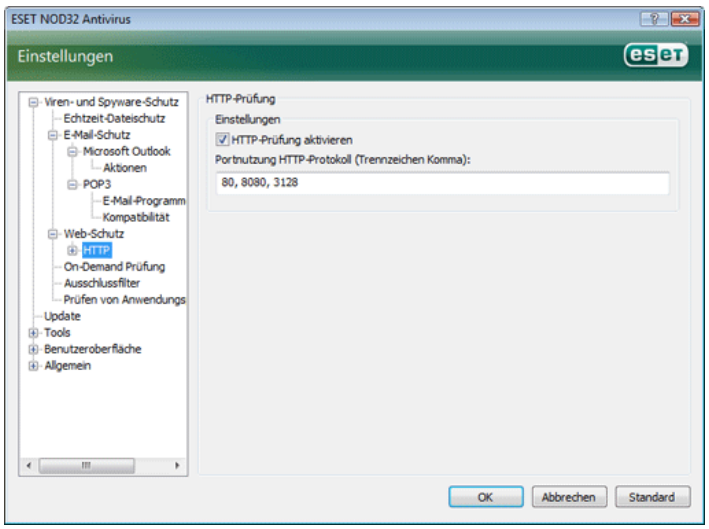
4.1.3 Web-Schutz

Die Internetverbindung ist eine Standardfunktion jedes Computers. doch leider ist diese auch der Hauptübertragungsweg für Schadcode. Daher ist es überaus wichtig, für einen ausreichenden Web-Schutz zu sorgen. Die Option **Web-Schutz aktivieren** sollte in jedem Fall aktiviert werden. Sie finden diese Option unter **Erweiterte Einstellungen (F5) > Virenschutz und Spywareschutz > Web-Schutz**.



4.1.3.1 HTTP

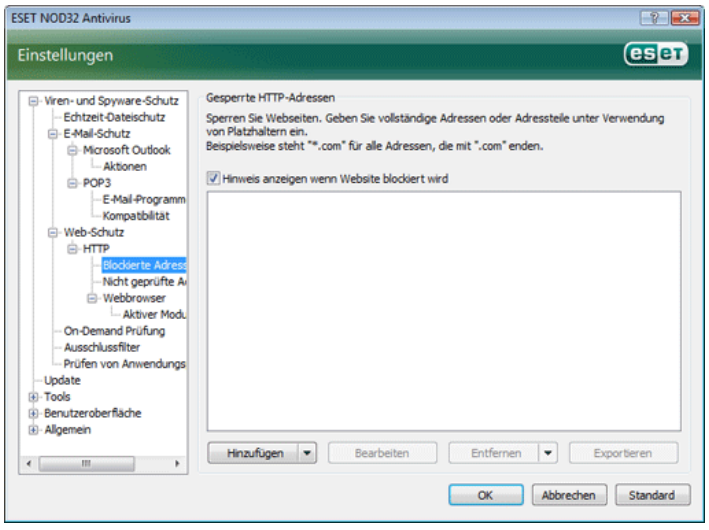
Der Web-Schutz besteht hauptsächlich in der Überwachung der HTTP-Kommunikation zwischen Webbrowsern und Servern im Internet. ESET NOD32 Antivirus ist standardmäßig für die HTTP-Standards der gängigen Webbrowser konfiguriert. Dennoch können Sie die Einstellungen für die HTTP-Prüfung im Abschnitt **Web-Schutz > HTTP** teilweise bearbeiten. Im Fenster **Einstellungen HTTP-Prüfung** können Sie die HTTP-Prüfung über die Option **HTTP-Prüfung aktivieren** aktivieren oder deaktivieren. Sie können auch die Portnummern definieren, die vom System für die HTTP-Kommunikation verwendet werden. In der Standardeinstellung werden die Portnummern 80, 8080 und 3128 verwendet. HTTP-Datenverkehr kann auf beliebigen Ports erkannt und geprüft werden. Geben Sie dazu weitere Portnummern ein, die durch ein Komma getrennt werden.



4.1.3.1.1 Blockierte/ausgeschlossene Adressen

In den Einstellungen für die HTTP-Prüfung können Sie benutzerdefinierte Listen für **blockierte** und **ausgeschlossene** URL (Uniform Resource Locator)-**Adressen** erstellen.

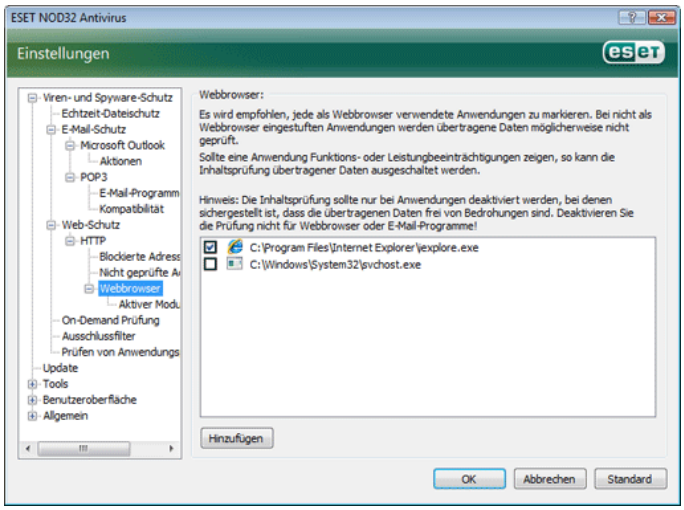
Beide Dialogfenster enthalten die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Exportieren**, über die Sie die Adresslisten auf einfache Weise verwalten können. Wenn die vom Benutzer angefragte Adresse in der Liste der blockierten Adressen aufgeführt wird, ist kein Zugriff auf diese Adresse möglich. Andererseits erfolgt der Zugriff auf Adressen, die in der Liste der ausgeschlossenen Adressen aufgeführt sind, ohne Prüfung auf Schadcode. In beiden Listen können die Sonderzeichen * (Sternchen) und **?** (Fragezeichen) verwendet werden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und **?** korrekt verwendet werden.



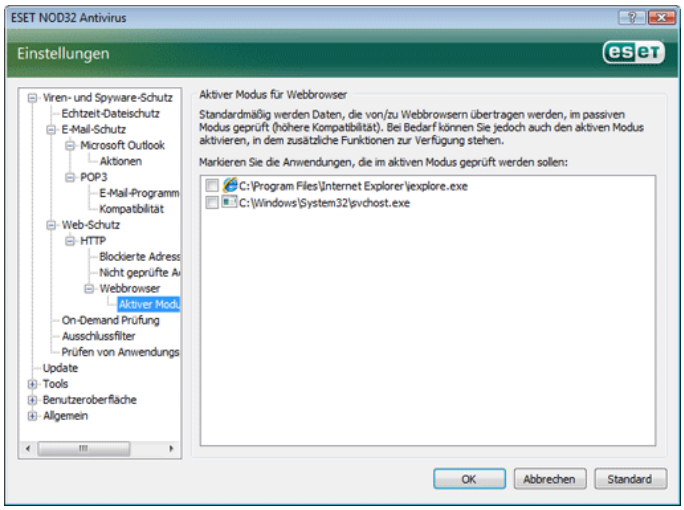
4.1.3.1.2 Webbrowser

Über die Funktion **Webbrowser** von ESET NOD32 Antivirus kann festgelegt werden, ob es sich bei einer bestimmten Anwendung um einen Browser handelt oder nicht. Wird eine Anwendung vom Benutzer als Browser eingestuft, wird die gesamte Kommunikation dieser Anwendung überwacht, und zwar unabhängig von den verwendeten Portnummern.

Die Webbrowser-Funktion ist eine Ergänzung der HTTP-Prüfung, da die HTTP-Prüfung nur für ausgewählte Ports durchgeführt wird. Viele Internetdienste verwenden jedoch sich dynamisch ändernde oder unbekannte Portnummern. Um diesem Sachverhalt Rechnung zu tragen, kann mithilfe der Webbrowser-Funktion die gesamte Portkommunikation unabhängig von den Verbindungsparametern überwacht werden.



Die Liste der Anwendungen, die als Browser eingestuft sind, kann im Bereich **HTTP** direkt über das Untermenü **Webbrowser** aufgerufen werden. Dieser Abschnitt enthält außerdem das Untermenü **Aktiver Modus**, in dem der Prüfungsmodus für die Webbrowser festgelegt wird. Die Funktion **Aktiver Modus** dient der Untersuchung der übertragenen Daten als Ganzes. Ist die Option nicht aktiviert, wird die Kommunikation der Anwendungen nur Stück für Stück überwacht. Dies verringert die Effizienz der Datenverifizierung, erhöht jedoch die Kompatibilität der aufgeführten Anwendungen. Wenn bei seiner Verwendung keine Probleme auftreten, sollten Sie den aktiven Modus aktivieren, indem Sie das Kontrollkästchen neben der gewünschten Anwendung aktivieren.



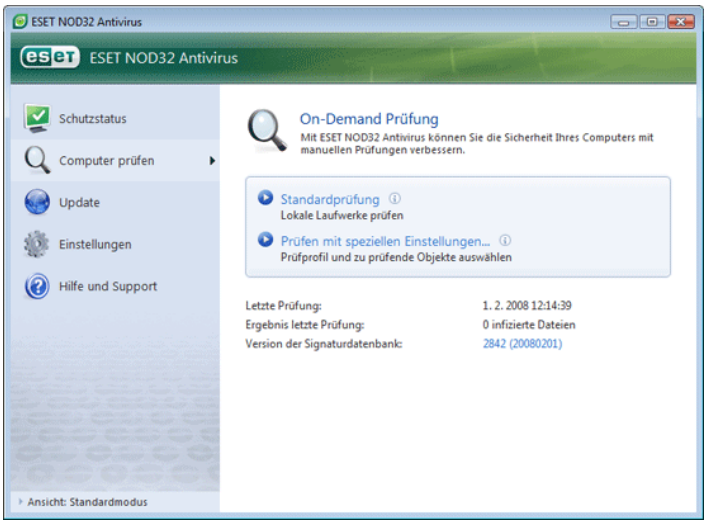
4.1.4 Computer prüfen

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), führen Sie eine manuelle -Prüfung aus, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Aus Sicherheitsgründen ist es dringend erforderlich, dass Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. Eine regelmäßige Prüfung dient der Erkennung von eingedrungener Schadsoftware, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der Schadsoftware nicht erkannt wurde. Dies kann passieren, wenn die Echtzeitprüfung- zur Zeit der Infektion deaktiviert war oder die Signaturdatenbank veraltet ist.

Sie sollten mindestens ein- bis zweimal im Monat eine manuelle Prüfung- vornehmen. Sie können die Prüfung als Task unter **Extras > Taskplaner** konfigurieren.

4.1.4.1 Prüfmethode

Es stehen zwei Methoden zur Auswahl. Bei der **Standardprüfung** wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Bei der Methode **Prüfen mit speziellen Einstellungen**... können Sie eines der vordefinierten Prüfprofile auswählen und die zu prüfenden Objekte in der Baumstruktur auswählen.



4.1.4.1.1 Standardprüfung

Die Standardprüfung ist eine -benutzerfreundliche Methode, mit der Benutzer einen Computer schnell prüfen und infizierte Dateien ohne weiteres Eingreifen entfernen können. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Bei der Standardprüfung werden alle Dateien auf den lokalen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt oder gelöscht. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Entfernungstypen finden Sie unter „Schadcode entfernen“ (siehe Seite 18).

Das Standardprofil ist für Benutzer gedacht, die ihren Computer schnell und einfach auf Viren prüfen möchten. Die Prüfung des Computers und das Entfernen der Schadsoftware mit dem Standardprofil ist effizient und erfordert keine ausführliche Konfiguration.

4.1.4.1.2 Prüfen mit speziellen Einstellungen

Über die Option „Prüfen mit speziellen Einstellungen“ können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden angeben. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Die Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden, die sinnvoll sind, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Um die zu prüfenden Objekte auszuwählen, verwenden Sie das Dropdown-Menü der Ziel-Schnellauswahl, oder wählen Sie die Objekte in der Baumstruktur aus, in der alle auf dem Computer verfügbaren Geräte aufgeführt werden. Außerdem können Sie zwischen drei Entfernungsstufen wählen. Klicken Sie dazu auf **Einstellungen... > Schadcode entfernen**. Wenn Sie das System ohne zusätzliche Aktionen prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**.

Das Prüfen mit speziellen Einstellungen eignet sich für fortgeschrittene Benutzer, die bereits Erfahrung mit Virenschutzprogrammen gesammelt haben.

4.1.4.2 Zu prüfende Objekte

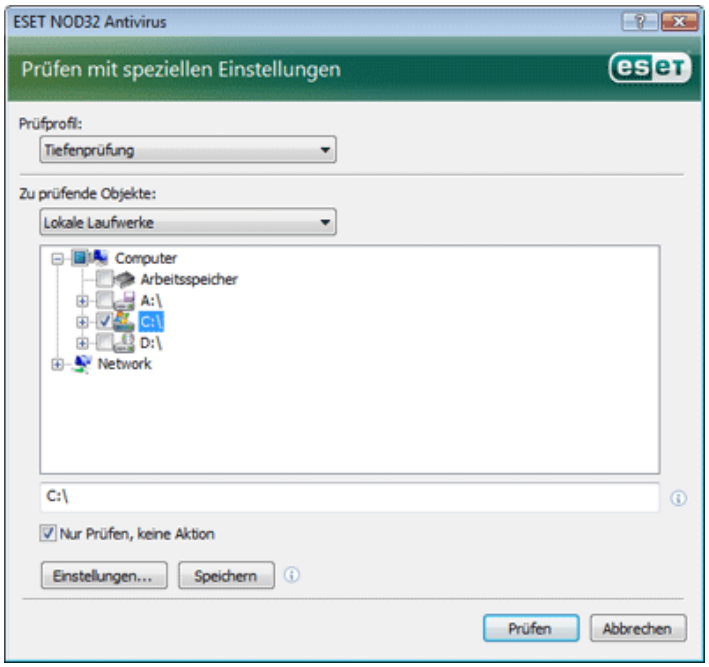
Über das Dropdown-Menü „Zu prüfende Objekte" werden die Dateien, Ordner und Geräte (Laufwerke) ausgewählt, die auf Viren geprüft werden sollen.

Über die Menüoption „Zu prüfende Objekte" können Sie die folgenden Objekte festlegen:

Lokale Laufwerke – Alle Festplatten des Systems werden geprüft

Wechselmedien – Disketten, USB-Speichergeräte, CD/DVD

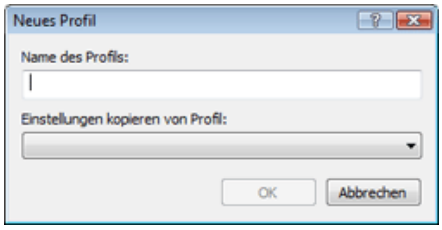
Netzlaufwerke – Alle verbundenen Netzlaufwerke



Sie können ein zu prüfendes Objekt auch genauer angeben, indem Sie den Pfad zum Ordner oder den Dateien eingeben, die geprüft werden sollen. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Geräte aufgelistet werden.

4.1.4.3 Prüfprofile

Die bevorzugten Parameter zum Prüfen Ihres Computers können als Profil gespeichert werden. Durch das Erstellen von Prüfprofilen können Sie dieselben Parameter in Zukunft regelmäßig wiederverwenden. Wir empfehlen Ihnen, nur solche Profile (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern) zu erstellen, die der Benutzer auch regelmäßig verwendet.



Um ein neues Profil zu erstellen, das wiederholt für Prüfungen eingesetzt werden kann, wählen Sie **Erweiterte Einstellungen** (F5) **> Manuelles -Prüfen des Computers**. Klicken Sie rechts auf die Schaltfläche **Profile...**, um die Liste vorhandener Prüfprofile anzuzeigen, und anschließend auf die Option zum Erstellen eines neuen Profils. Die folgenden **Einstellungen für ThreatSense** beschreiben jeden Parameter der Prüfeinstellungen. Auf diese Weise können Sie ein Prüfprofil erstellen, das Ihren Anforderungen gerecht wird.

Beispiel:
Angenommen, Sie möchten Ihr eigenes Prüfprofil erstellen und halten die Konfiguration des Profils **Smart Scan** für teilweise geeignet. Sie möchten jedoch keine laufzeitkomprimierten Dateien oder potenziell unsicheren Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Klicken Sie im Fenster **Konfigurationsprofile** auf **Hinzufügen...**. Geben Sie den Namen des neuen Profils im Feld **Profilname** ein, und wählen Sie im Dropdown**Menü Einstellungen kopieren von Profil:** ***die Option*** Smart Scan- aus. Passen Sie anschließend die übrigen Parameter Ihren eigenen Erfordernissen an.

4.1.5 Einstellungen für ThreatSense

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Eingesetzt wird eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen, Virussignaturen), die zusammen die Systemsicherheit deutlich erhöhen. Die Prüf-Engine kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch Rootkits erfolgreich.

In den Einstellungen für ThreatSense kann der Benutzer verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Entfernungsstufen usw.

Um das Fenster für die Einstellungen zu öffnen, klicken Sie auf die Schaltfläche **Einstellungen...**, die im Fenster aller Module, die ThreatSense verwenden, angezeigt wird (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- Echtzeit-Dateischutz
- Prüfung Systemstartdateien
- E-Mail-Schutz
- Web-Schutz
- Manuelle -Prüfung

Die ThreatSense-Parameter sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der erweiterten Heuristik im Modul Echtzeit-Dateischutz dazu führen, dass das System langsamer -arbeitet (normalerweise werden mit diesen Methoden nur neu -erstellte Dateien geprüft). Es wird daher empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Prüfen des Computers" vorgenommen werden.

4.1.5.1 Einstellungen für zu prüfende Objekte

Im Bereich **Objekte** können Sie festlegen, welche Computerkomponenten und Dateien auf Schadcode geprüft werden sollen.

Arbeitsspeicher – Prüfung des Arbeitsspeichers auf mögliche Bedrohungen

Boot-Sektoren – Prüfung der Boot-Sektoren auf Viren im Master Boot Record

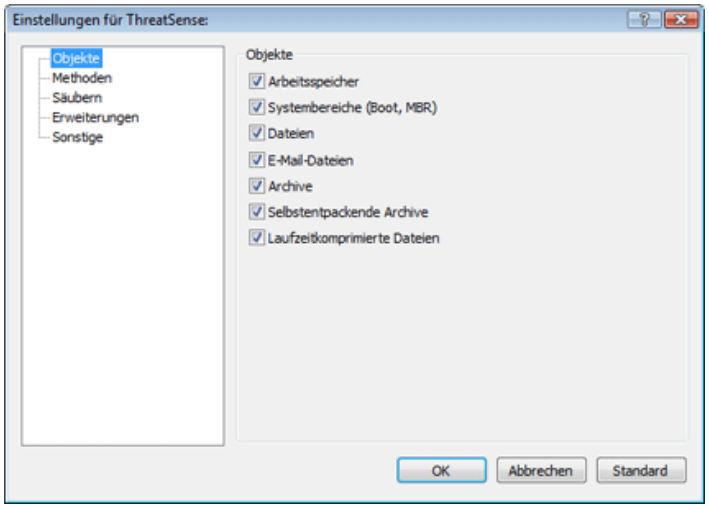
Dateien – Prüfung der gängigen Dateitypen (Programm-, Bild-, Audio-, Video-, Datenbankdateien usw.)

E-Mail-Dateien – Prüfung von Dateien, die E-Mail-Nachrichten enthalten

Archives – Prüfung von komprimierten Archivdateien (RAR, ZIP, ARJ, TAR, usw.)

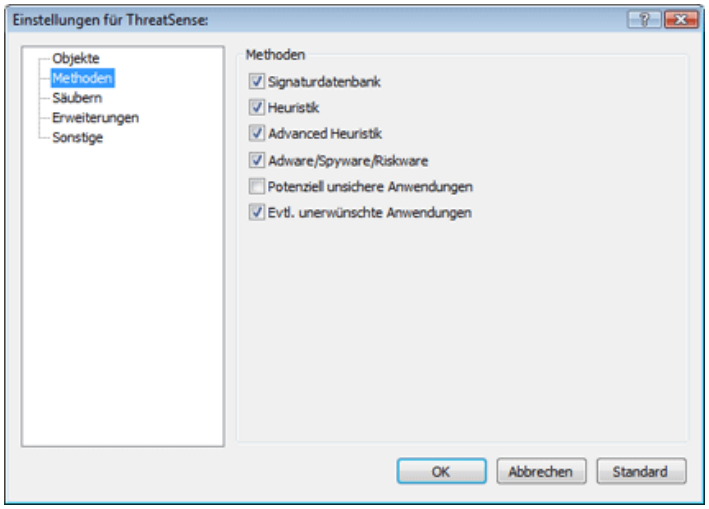
Selbstentpackende -Archive – Prüfung von Dateien in selbstentpackenden -Archiven, liegen in der Regel mit der Erweiterung „.exe" vor

Laufzeitkomprimierte Dateien – Laufzeitkomprimierte Dateien (anders als Standard-Archivtypen) werden im Arbeitsspeicher dekomprimiert, zusätzlich zu statisch laufzeitkomprimierten Dateien (UPX, yoda, ASPack, FGS etc.).



4.1.5.2 Optionen

Im Bereich **Optionen** können Sie die Methoden für die System-Schadsoftwareprüfung auswählen. Folgende Optionen stehen zur Verfügung:



Signaturen – Mithilfe von Signaturen kann Schadsoftware zuverlässig anhand des Namens erkannt und identifiziert werden.

Heuristik – Als heuristische Methoden werden Verfahren bezeichnet, die (bösartige) Aktivitäten von Programmen analysieren. Mit ihrer Hilfe können bis dato unbekannte bösartige Programme oder Viren, die nicht in der Liste bekannter Viren (Signaturdatenbank) aufgeführt waren, erkannt werden.

Erweiterte Heuristik – Als erweiterte Heuristik werden besondere heuristische Verfahren bezeichnet, die von ESET entwickelt wurden, um Würmer und Trojaner zu erkennen, die in höheren Programmiersprachen geschrieben wurden. Dank erweiterter Heuristik-Funktionen werden die Erkennungsmethoden noch ausgefeilter.

Adware/Spyware/Riskware – Diese Kategorie umfasst Software zum Ausspionieren von vertraulichen Benutzerinformationen. Dazu zählt auch Software zum Anzeigen von Werbebannern.

Potenziell unsichere Anwendungen – Unter dieser Bezeichnung werden Programme zusammengefasst, die zwar erwünscht sind, aber Funktionen bereitstellen, die potenziell gefährlich sein können. Da hierzu auch Programme für das Fernsteuern von Computern gehören, ist diese Option standardmäßig deaktiviert.

Eventuell unerwünschte Anwendungen – Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die nicht unbedingt Sicherheitsrisiken mit sich bringen, aber Auswirkungen auf Leistung und Verhalten Ihres Computers haben. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Dazu zählen vor allem ungewollte Popup-Fenster, die Aktivierung und Ausführung versteckter Prozesse, die erhöhte Inanspruchnahme von Systemressourcen, Änderungen in Suchergebnissen sowie die Kommunikation von Anwendungen mit Remote-Servern.

4.1.5.3 Schadcode entfernen

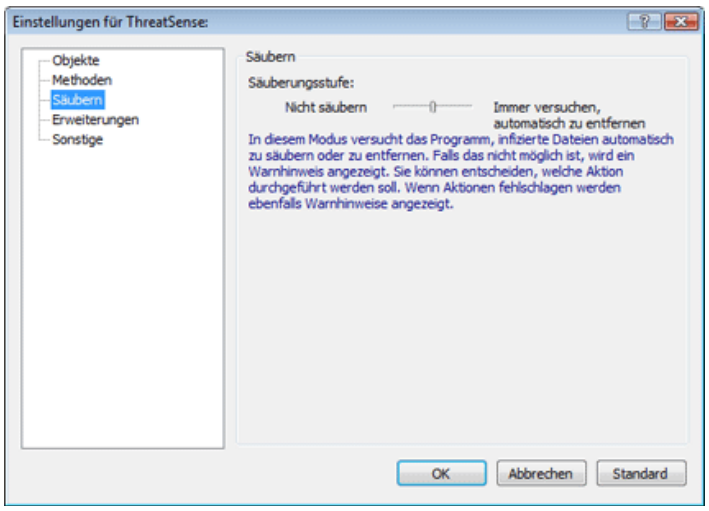
Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt 3 Arten der Schadcodeentfernung:

Nicht säubern
Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen.

Standardmodus
Das Programm versucht, den Schadcode aus der Datei zu entfernen oder die infizierte Datei zu löschen. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine -Aktion auszuwählen. Diese -Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.

Immer versuchen, automatisch zu entfernen
Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht die Dateien (einschließlich Archive). Ausnahmen gelten nur für Systemdateien. Wenn es nicht möglich ist, den Schadcode zu entfernen, wird der Benutzer aufgefordert, eine Aktion auszuwählen.

Warnung:
Im Standardmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Wenn es auch nicht infizierte Dateien enthält, wird die Archivdatei nicht gelöscht. Wenn die Option „Immer versuchen, automatisch zu entfernen" aktiviert ist, wird die Archivdatei gelöscht, sobald eine einzige Datei im Archiv infiziert ist.


Einstellungen für ThreatSense:
Objekte
Methoden
Säubern
Erweiterungen
Sonstige
Säubern
Säuberungsstufe:
Nicht säubern
Immer versuchen, automatisch zu entfernen
In diesem Modus versucht das Programm, infizierte Dateien automatisch zu säubern oder zu entfernen. Falls das nicht möglich ist, wird ein Warnhinweis angezeigt. Sie können entscheiden, welche Aktion durchgeführt werden soll. Wenn Aktionen fehlschlagen werden ebenfalls Warnhinweise angezeigt.
OK
Abbrechen
Standard

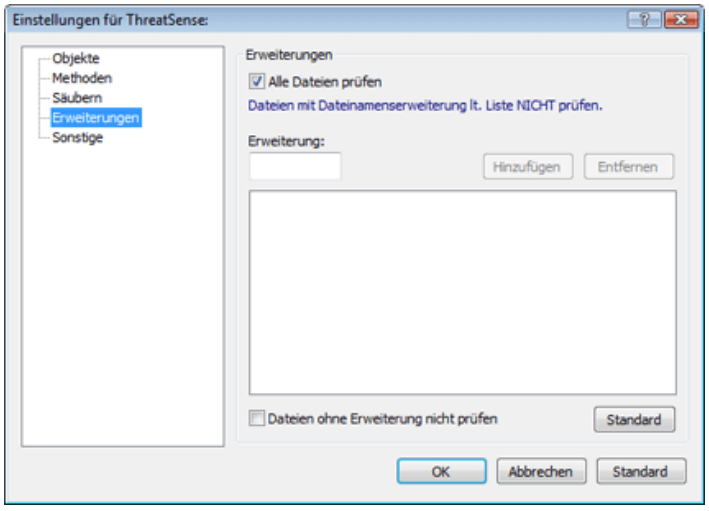
4.1.5.4 Dateierweiterungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt der Datei. In diesem Abschnitt der ThreatSense-Einstellungen werden Sie die Dateitypen festlegen, die geprüft werden sollen.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung geprüft. Jede Erweiterung kann der Liste ausgeschlossener Dateien hinzugefügt werden. Wenn die Option **Alle Dateien prüfen** nicht aktiviert ist, werden in der Liste alle gegenwärtig geprüften Dateierweiterungen angezeigt. Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen geprüft werden sollen.

Um die Prüfung von Dateien ohne Erweiterung zu aktivieren, aktivieren Sie die Option **Dateien ohne Erweiterung prüfen**.

Der Ausschluss bestimmter Dateien ist dann angebracht, wenn die Prüfung bestimmter Dateitypen zu Fehlern bei der Ausführung der zuständigen Programme führt. So sollten Sie z. B. die Erweiterungen „.edb", „.eml" und „.tmp" ausschließen, wenn Sie MS Exchange Server verwenden.



4.1.6 Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Webseiten, gemeinsame Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, Disketten usw.).

Wenn Ihr Computer Symptome einer Infektion mit Schadsoftware aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

- Starten Sie ESET NOD32 Antivirus, und klicken Sie auf **Computer prüfen**
- Klicken Sie auf Standardprüfung (weitere Informationen finden Sie unter „Standardprüfung").
- Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und wiederhergestellten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Prüfen mit speziellen Einstellungen**, und wählen Sie die Bereiche aus, die auf Viren geprüft werden sollen.

Das folgende allgemeine Beispiel soll veranschaulichen, wie in ESET Smart Security mit Schadsoftware umgegangen wird. Nehmen wir einmal an, die Echtzeit-Systemüberwachung verwendet die Standard-Entfernungsstufe und erkennt eingedrungene Schadsoftware. Im Folgenden wird der Versuch gestartet, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeit-Schutz keine vordefinierte Aktion angegeben, müssen Sie in einem Warnungsfenster zwischen verschiedenen Optionen wählen. In der Regel stehen die Optionen **Schadcode entfernen**, **Löschen** und **Belassen** zur Auswahl. Es wird nicht empfohlen, die Option **Belassen** zu wählen, da sonst die infizierten Dateien nicht behandelt werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.

Schadcode entfernen und löschen
Wenden Sie „Schadcode entfernen" an, wenn eine „saubere" Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn eine infizierte Datei „gesperrt" ist oder von einem Systemprozess verwendet wird, muss die Datei in der Regel erst freigegeben werden (häufig ist dazu ein Systemneustart erforderlich), bevor sie gelöscht werden kann.

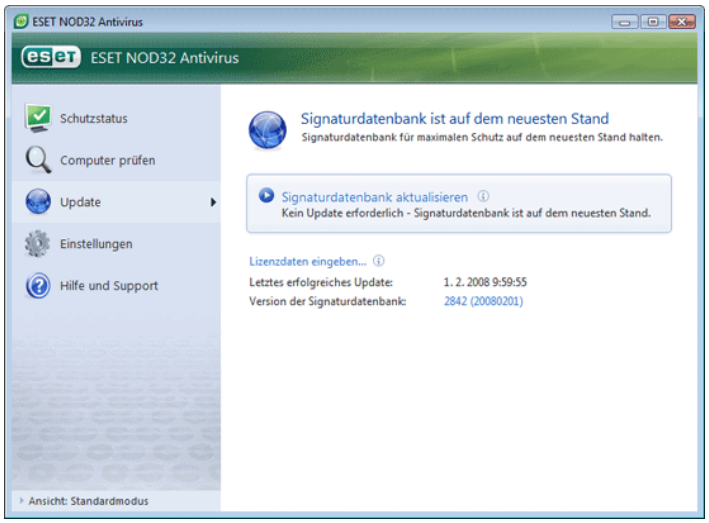
Dateien in Archiven löschen
Im Standardmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. In anderen Worten: Im Standardmodus werden Archive nicht gelöscht, wenn sie zusätzlich nicht infizierte Dateien enthalten. Die Option „Immer versuchen, automatisch zu entfernen" sollten Sie allerdings mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und dies unabhängig vom Status der übrigen Archivdateien.

4.2 Programm aktualisieren

Eine regelmäßige Aktualisierung des Programms ist die grundlegende Voraussetzung, damit ESET Smart Security den größtmöglichen Schutz bieten kann. Mit dem Update-Modul wird gewährleistet, dass das Programm stets auf dem neuesten Stand ist. Dabei werden zwei Methoden kombiniert – die Aktualisierung der Signaturdatenbank und die Aktualisierung der Systemkomponenten.

Informationen über den aktuellen Update-Status finden Sie unter der Option **Update**. Dort werden Informationen zur aktuellen Version der Signaturdatenbank angezeigt, und Sie sehen, ob eine Aktualisierung erforderlich ist. Darüber hinaus kann an dieser Stelle auch der Update-Vorgang sofort gestartet werden. Nutzen Sie dazu die Option **Update der Signaturdatenbank** . Außerdem können Sie grundlegende Einstellungen für Updates vornehmen, z. B. den Benutzernamen und das Passwort für die Update-Server von ESET eintragen.

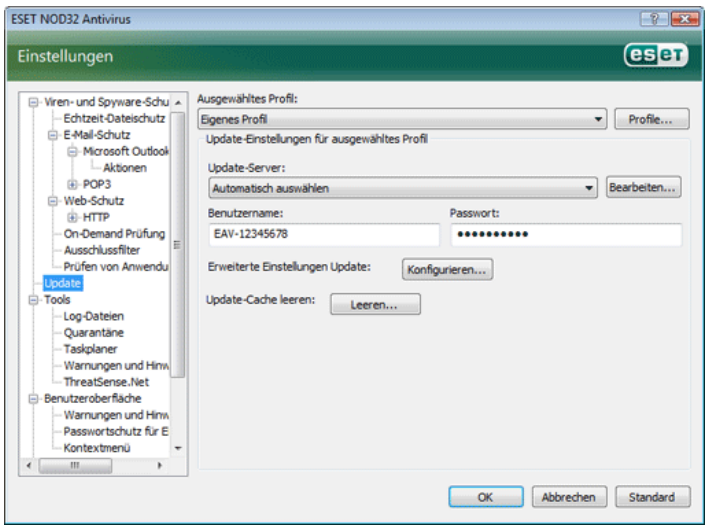
Im Informationsfenster werden weitere Details wie das Datum und die Uhrzeit des letzten erfolgreichen Updates und die Nummer der Signaturdatenbank angezeigt. Diese Nummer ist ein aktiver Link zur Website von ESET, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.



HINWEIS: Sie erhalten den Benutzernamen und das Passwort von ESET nach dem Kauf von ESET Smart Security.

4.2.1 Einstellungen für Updates

In den Einstellungen für Updates finden Sie Informationen zum Ursprung von Updates, z. B. die Liste der Update-Server und die Authentifizierungsdaten für diese Server. Standardmäßig ist im Feld **Update-Server:** die Option **Automatisch auswählen** festgelegt. Mit dieser Option wird gewährleistet, dass Update-Dateien automatisch von den ESET-Update-Servern heruntergeladen werden und gleichzeitig der Netzwerk-Datenverkehr der einzelnen Update-Server berücksichtigt wird. Die Einstellungen für Updates finden Sie in den erweiterten Einstellungen (F5) unter **Update**.



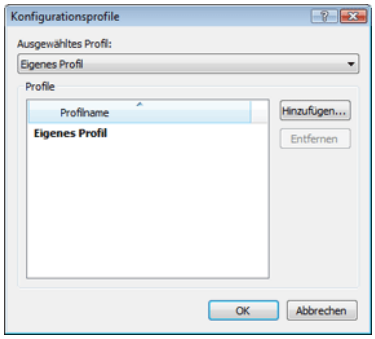
Die Liste der aktuellen Update-Server kann im Dropdown -**Menü unter** Update-Server: aufgerufen werden. Um einen neuen Update-Server hinzuzufügen, klicken Sie im Bereich **Update-Einstellungen für ausgewähltes Profil** auf **Bearbeiten...**. Klicken Sie anschließend auf **Hinzufügen**.

Zur Authentifizierung müssen der **Benutzername** und das **Passwort** eingeben werden, die Sie nach dem Kauf der ESET-Produktlizenz erhalten haben.

4.2.1.1 Update-Profile

Für verschiedene Update-Konfigurationen können benutzerdefinierte Update-Profile erstellt werden, die für bestimmte Update-Tasks verwendet werden. Besonders sinnvoll ist das Erstellen verschiedener Update-Profile für mobile Benutzer, bei denen sich bei der Internetverbindung häufig Änderungen ergeben. Mobile Benutzer können den Update-Task so ändern, dass anstelle der unter **Mein Profil** angegebenen Konfiguration ein alternatives Profil verwendet wird, wenn ein Update mit dem ersten Profil nicht möglich ist.

Im Dropdown-Menü **Ausgewähltes Profil** wird das gegenwärtig verwendete Profil angezeigt. Standardmäßig ist dies **Mein Profil**. Zum Erstellen eines neuen Profils klicken Sie auf **Profile...** und dann auf **Hinzufügen...**. Geben Sie anschließend den **Namen des Profils** ein. Beim Erstellen eines neuen Profils können Sie über **Einstellungen kopieren von Profil:** die Einstellungen eines vorhandenen Profils übernehmen.



In den Profileinstellungen können Sie den Update-Server angeben, zu dem das Programm eine Verbindung für den Download von Updates herstellt. Dies kann ein beliebiger Server aus der Liste der verfügbaren Server oder ein neu hinzugefügter Server sein. Die Liste der vorhandenen Update-Server kann im Dropdown-**Menü unter** Update-Server: aufgerufen werden. Um einen neuen Update-Server hinzuzufügen, klicken Sie im Bereich **Update-Einstellungen für ausgewähltes Profil auf** Bearbeiten.... Klicken Sie anschließend auf **Hinzufügen**.

4.2.1.2 Erweiterte Einstellungen für Updates

Um **Erweiterte Einstellungen Update** anzuzeigen, klicken Sie auf **Einstellungen...**. Zu den erweiterten Einstellungen gehören Optionen für **Update-Modus, HTTP-Proxy, LAN** und **Update-Mirror**.

4.2.1.2.1 Update-Modus

Auf der Registerkarte **Update-Modus** finden Sie Optionen zum Aktualisieren der Programmkomponenten.

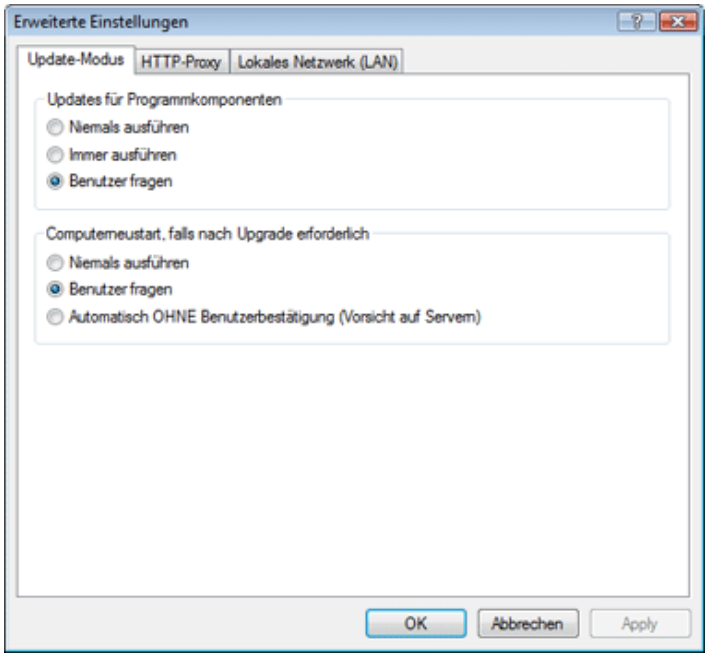
Im Abschnitt **Updates für Programmkomponenten** stehen drei Optionen zur Verfügung:

- **Programmkomponenten nicht aktualisieren**
- **Immer ausführen**
- **Benutzer fragen**

Wenn Sie die Option **Programmkomponenten nicht aktualisieren** wählen, werden neue Updates für Programmkomponenten, die von ESET veröffentlicht wurden, nicht heruntergeladen, und auf dem entsprechenden Computer erfolgt keine Aktualisierung von Programmkomponenten. Wenn Sie die Option **Programmkomponenten automatisch aktualisieren** wählen, werden Updates für Programmkomponenten immer ausgeführt, sobald ein neues Update auf den ESET-Update-Servern verfügbar ist, und die entsprechende Programmkomponente wird durch das Herunterladen der neuen Version aktualisiert.

Wählen Sie die dritte Option, **Benutzer fragen**, wenn Sie das Herunterladen neu verfügbarer Updates zuvor durch den Benutzer bestätigen lassen möchten. In diesem Fall wird ein Dialogfenster mit Informationen zum verfügbaren Update angezeigt, und der Benutzer kann entscheiden, ob das Update bestätigt oder abgelehnt werden soll. Nach der Bestätigung wird das Update heruntergeladen, und die neuen Programmkomponenten werden anschließend installiert.

Die Standardoption für Updates für Programmkomponenten ist **Benutzer fragen**.



Nach der Installation eines Updates für Programmkomponenten ist ein Neustart des Systems erforderlich, um die Funktionalität aller Module zu gewährleisten. Im Bereich **Neustart nach Update von Programmkomponenten** kann der Benutzer eine der folgenden drei Optionen auswählen:

- **Kein Neustart**
- **Zur Bestätigung auffordern**
- **Computer automatisch neu starten, ohne Nachfrage**

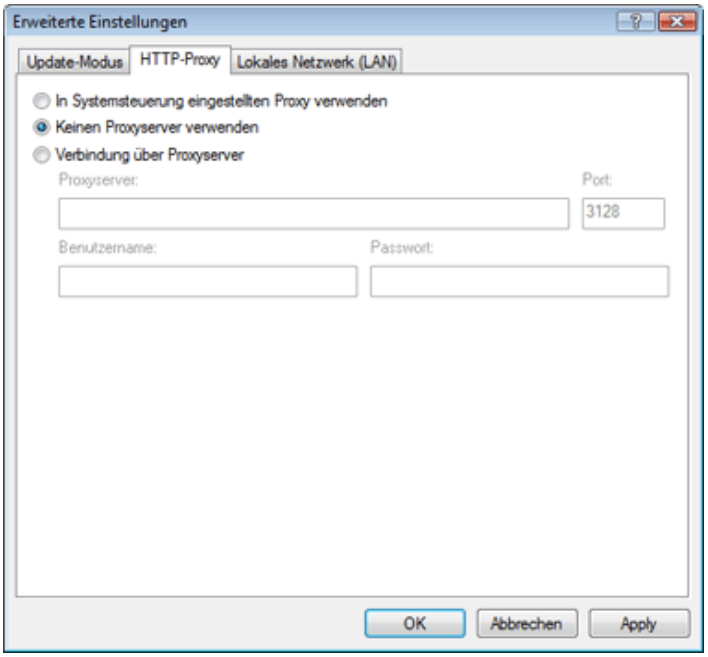
Die Standardeinstellung für den Neustart ist **Zur Bestätigung auffordern**. Die Auswahl der geeigneten Option für Updates für Programmkomponenten auf der Registerkarte **Update-Modus** hängt vom jeweiligen Computer ab, auf dem die Einstellungen zugewiesen werden. Beachten Sie die unterschiedliche Funktion von Arbeitsplatzcomputern und Servern – das automatische Neustarten eines Servers nach einem Update kann schwerwiegende Folgen haben.

4.2.1.2.2 Proxyserver

Um auf die Proxyserver-Einstellungen für ein bestimmtes Update-Profil zuzugreifen, klicken Sie in den erweiterten Einstellungen (F5) auf **Update** und dann auf **Einstellungen...** rechts neben den **erweiterten Update-Einstellungen.** Klicken Sie auf die Registerkarte **HTTP-Proxy**, und wählen Sie eine der folgenden drei Optionen:

- **Allgemeine Einstellungen für den Proxyserver verwenden**
- **Keinen Proxyserver verwenden**
- **Verbindung über Proxyserver** (Verbindung wird durch Verbindungseigenschaften definiert)

Bei Auswahl der Option **Allgemeine Einstellungen für den Proxyserver verwenden** werden die Proxyserver-Konfigurationsoptionen verwendet, die in den erweiterten Einstellungen unter **Allgemein > Proxyserver** angegeben wurden.



Wählen Sie die Option **Keinen Proxyserver verwenden**, wenn Sie festlegen möchten, dass kein Proxyserver für die Aktualisierung von ESET Smart Security verwendet werden soll.

Die Option **Verbindung über Proxyserver** sollte gewählt werden, wenn für die Aktualisierung von ESET NOD32 Antivirus ein anderer Proxyserver als der in den allgemeinen Einstellungen (**Allgemein > Proxyserver**) angegebene verwendet wird. In diesem Fall sind weitere Einstellungen erforderlich: **Proxyserver**-Adresse, der **Port** für die Datenübertragung sowie **Benutzername** und **Passwort** für den Proxyserver, falls erforderlich.

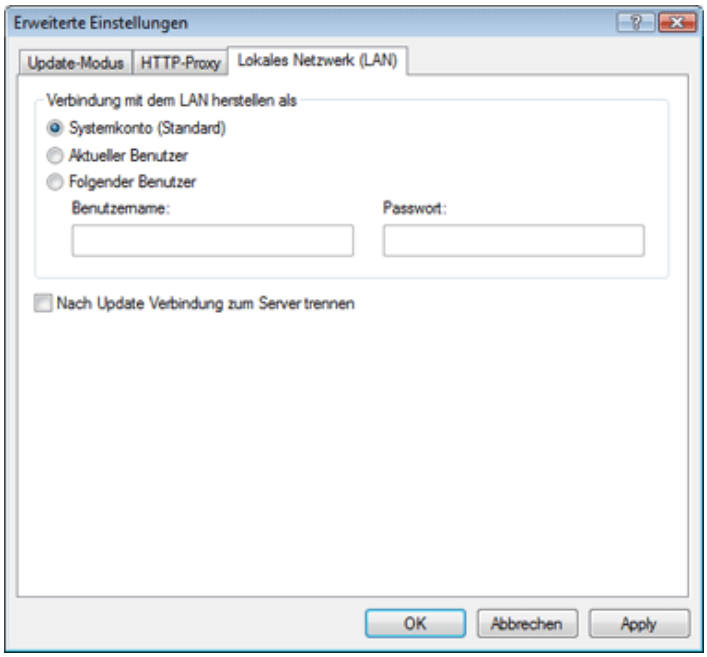
Diese Option sollte auch verwendet werden, wenn in den allgemeinen Einstellungen kein Proxyserver festgelegt wurde, ESET NOD32 Antivirus jedoch die Verbindung über einen Proxyserver aufbaut.

Die Standardeinstellung für den Proxyserver ist **Allgemeine Einstellungen für den Proxyserver verwenden**.

4.2.1.2.3 LAN-Verbindungen

Beim Aktualisieren von einem lokalen Server unter Windows NT -ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich. In den meisten Fällen besitzt ein lokales Systemkonto keine ausreichenden Berechtigungen für den Zugriff auf den Mirror-Ordner (der Kopien der Update-Dateien enthält). Geben Sie in diesem Fall den Benutzernamen und das Passwort in den Update-Einstellungen ein, oder geben Sie ein Konto an, über das das Programm auf den Update-Mirror zugreifen kann.

Um ein solches Konto zu konfigurieren, klicken Sie auf die Registerkarte **LAN**. Der Bereich **Verbindung mit dem LAN herstellen als** enthält die Optionen **Systemkonto (Standardeinstellung)**, **Aktueller Benutzer** und **Folgender Benutzer**.



Wählen Sie **Systemkonto**, um das Systemkonto für die Authentifizierung zu verwenden. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Authentifizierungsdaten angegeben sind.

Um sicherzustellen, dass das Programm sich mit dem Konto eines aktuell -angemeldeten Benutzers autorisiert, wählen Sie **Aktueller Benutzer**. Nachteil dieser Lösung ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.

Wählen Sie **Folgender Benutzer**, wenn das Programm ein spezielles Benutzerkonto für die Authentifizierung verwenden soll.

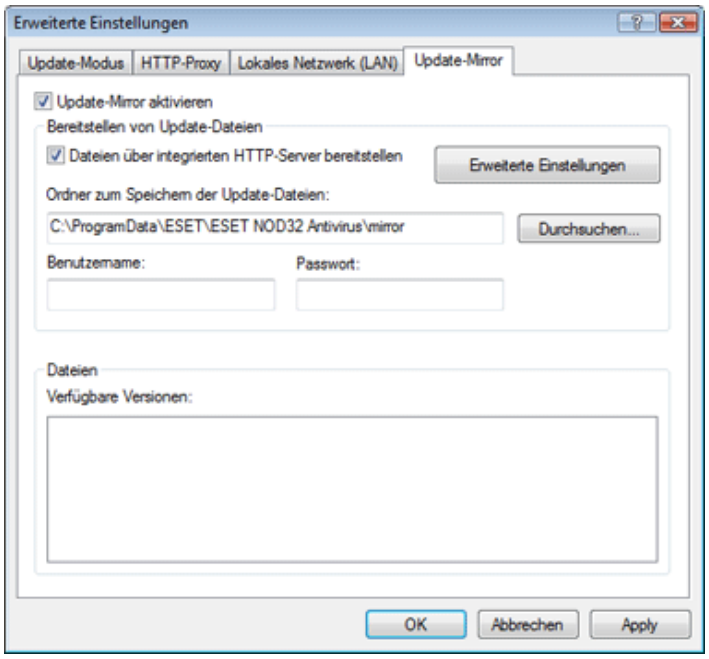
Die Standardeinstellung für LAN-Verbindungen ist **Systemkonto**.

Warnung:
Wenn eine der Optionen **Aktueller Benutzer** oder **Folgender Benutzer**aktiviert ist, kann beim Wechsel der Identität zum gewünschten Benutzer ein Fehler auftreten. Aus diesem Grund wird empfohlen, die LAN-Authentifizierungsdaten in den Haupteinstellungen für Updates einzugeben. In diesen Update-Einstellungen geben Sie die Authentifizierungsdaten wie folgt ein: Domain-Name\Benutzer (bei einer Arbeitsgruppe geben Sie Arbeitsgruppenname\Name ein) und das Benutzerpasswort. Bei der Aktualisierung von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

4.2.1.2.4 Erstellen von Update-Kopien – Update-Mirror

Mit ESET NOD32 Antivirus Business Edition können Kopien der Update-Dateien erstellt werden, die für die Aktualisierung anderer Computer im Netzwerk verwendet werden können. Das Aktualisieren der Clientcomputer von einem Update-Mirror sorgt für eine optimierte Lastenverteilung im Netzwerk sowie eine Reduzierung der benötigten Bandbreiten.

Die Konfigurationsoptionen für den Update-Mirror des lokalen Servers befinden sich im Bereich **Erweiterte Einstellungen Update**. (Dafür müssen Sie zunächst im Lizenzmanager, der sich im Bereich „Erweiterte Einstellungen" von ESET Smart Security Business Edition öffnen lässt, einen gültigen Lizenzschlüssel eingeben. Um auf diesen Bereich zuzugreifen, drücken Sie F5, und klicken Sie unter „Erweiterte Einstellungen" auf **Update**. Klicken Sie auf die Schaltfläche **Einstellungen...** neben **Erweiterte Einstellungen Update:**, und wählen Sie die Registerkarte **Update-Mirror**).



Der erste Schritt bei der Konfiguration des Update-Mirror besteht in der Aktivierung des Kontrollkästchens **Update-Mirror aktivieren**. Durch das Aktivieren dieser Option stehen weitere Konfigurationsoptionen für Update-Mirror zur Verfügung, die beispielsweise die Art des Zugriffs auf Update-Dateien und den Pfad zu den Kopien der Update-Dateien betreffen.

Die Vorgehensweise zur Aktivierung des Update-Mirror wird im folgenden Kapitel, „Aktualisieren über Update-Mirror", ausführlich beschrieben. Vorläufig sei angemerkt, dass es zwei Grundvarianten des Zugriffs auf den Update-Mirror gibt: Der Ordner mit den Update-Dateien kann eine Netzwerkfreigabe sein, oder es wird ein HTTP-Server als Update-Mirror verwendet.

Der den Update-Dateikopien vorbehaltene Ordner wird im Bereich **Speicherordner für Kopien der Update-Dateien** festgelegt. Klicken Sie auf **Durchsuchen...**, um den gewünschten Ordner auf dem lokalen Computer oder eine Netzwerkfreigabe auszuwählen. Wenn für den angegebenen Ordner eine Authentifizierung erforderlich ist, müssen die Authentifizierungsdaten in die Felder **Benutzername** und **Passwort** eingetragen werden. Der Benutzername muss im Format *Domain/Benutzer* oder *Arbeitsgruppe/Benutzer* eingegeben werden. Denken Sie daran, auch die entsprechenden Passwörter einzugeben.

In den erweiterten Einstellungen für Update-Mirror kann auch die Sprachversion der herunterzuladenden Update-Kopien angegeben

werden. Zum Auswählen der Sprache wechseln Sie zu **Dateien – Verfügbare Versionen**.

4.2.1.2.4.1 Aktualisieren über Update-Mirror

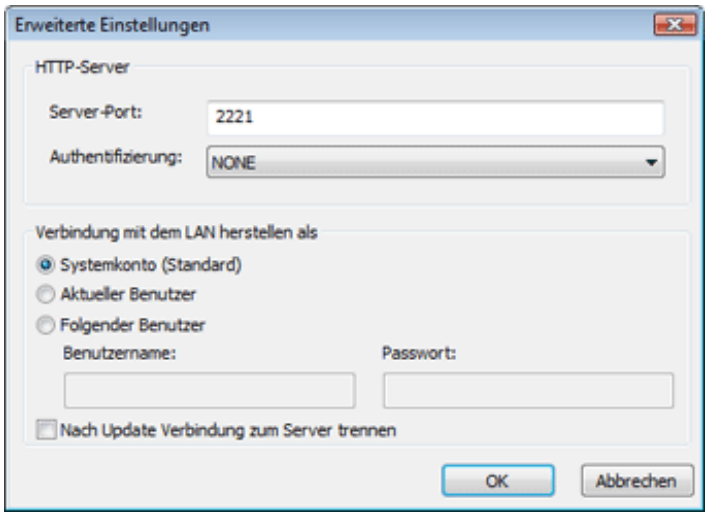
Es gibt zwei Grundvarianten für den Zugriff auf den Update-Mirror: Der Ordner mit den Update-Dateien kann eine Netzwerkfreigabe sein, oder es wird ein HTTP-Server als Update-Mirror verwendet.

Zugriff auf den Update-Mirror über einen internen HTTP-Server

Dies ist die in der vordefinierten Programmkonfiguration festgelegte Standardkonfiguration. Um mit dem HTTP-Server auf den Update-Mirror zugreifen zu können, wechseln Sie zu **Erweiterte Einstellungen Update** (Registerkarte **Update-Mirror**), und markieren Sie die Option **Update-Mirror aktivieren**.

In den **erweiterten Einstellungen** des **Update-Mirror** können Sie den **Server-Port** angeben, auf dem der HTTP-Server Anfragen empfängt, und den Typ der **Authentifizierung** festlegen, die vom HTTP-Server verwendet wird. Standardmäßig weist der Server-Port den Wert **2221** auf. Mit der Option **Authentifizierung** können Sie die für den Zugriff auf die Update-Dateien verwendete Authentifizierungsmethode wählen. Folgende Optionen stehen zur Verfügung: **KEINE, Basic** und **NTLM**. Wählen Sie **Basic** für Base64-Verschlüsselung und einfache Authentifizierung mit Benutzernamen und Passwort. Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat. Die Standardeinstellung ist **KEINE**, bei der für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

Warnung:
Wenn Sie den Zugriff auf die Update-Dateien über einen HTTP-Server zulassen möchten, muss sich der Ordner mit den Kopien der Update-Dateien auf demselben Computer befinden wie die Instanz von ESET NOD32 Antivirus, mit der dieser Ordner erstellt wird.



Wenn die Konfiguration des Update-Mirror abgeschlossen ist, fügen Sie auf den einzelnen Computern einen neuen Update-Server hinzu. Das Format lautet: **http://IP-Adresse_Ihres_Servers:2221**. Führen Sie dazu die folgenden Schritte aus:

- Öffnen Sie die **Erweiterten Einstellungen** von ESET NOD32 Antivirus, und klicken Sie auf **Update**.
- Klicken Sie rechts neben dem Dropdown-Menü **Update-Server** auf **Bearbeiten...**, und geben Sie den neuen Server im folgenden Format ein: http://IP-Adresse_Ihres_Servers:2221
- Wählen Sie den neu -hinzugefügten Server aus der Liste der Update-Server aus.

Zugriff auf den Update-Mirror über Systemfreigaben

Zunächst muss in einem lokalen oder Netzwerklaufwerk ein freigegebener Ordner erstellt werden. Beim Erstellen des Ordners für den Update-Mirror ist Folgendes zu beachten: Der Benutzer, der Update-Dateien im Ordner speichert, benötigt Schreibzugriff, während die Benutzer, die ESET NOD32 Antivirus über diesen Ordner aktualisieren, eine Leseberechtigung benötigen.

Die Konfiguration des Zugriffs auf den Update-Mirror wird fortgesetzt, indem Sie im Bereich **Erweiterte Einstellungen Update** (Registerkarte **Update-Mirror**) die Option **Dateien bereitstellen über integrierten HTTP-Server** deaktivieren. Diese Option ist in der Standardeinstellung des Programms aktiviert.

Wenn sich der freigegebene Ordner auf einem anderen Computer im Netzwerk befindet, ist für den Zugriff auf diesen Computer eine Authentifizierung erforderlich. Um die Authentifizierungsdaten anzugeben, wechseln Sie in die erweiterten Einstellungen von ESET NOD32 Antivirus (mit F5) und klicken auf **Update**. Klicken Sie auf **Einstellungen...** und anschließend auf die Registerkarte **LAN**. Diese Einstellung entspricht der Einstellung für Updates, wie im Kapitel „Herstellen einer LAN-Verbindung" beschrieben.

Nach Abschluss der Konfiguration des Update-Mirror geben Sie auf den einzelnen Computern jeweils \\UNC\\PATH als Update-Server ein. Führen Sie dazu die folgenden Schritte aus:

- Öffnen Sie die erweiterten Einstellungen von ESET NOD32 Antivirus, und klicken Sie auf **Update**.
- Klicken Sie neben dem Update-Server auf **Bearbeiten...**, und geben Sie den neuen Server im folgenden Format ein: \\UNC\PATH.
- Wählen Sie den neu -hinzugefügten Server aus der Liste der Update-Server aus.

HINWEIS: Um ein fehlerfreies Funktionieren zu gewährleisten, muss der Pfad zum Ordner mit den Kopien der Update-Dateien als UNC-Pfad angegeben werden. Updates über verbundene Netzlaufwerke funktionieren möglicherweise nicht.

4.2.1.2.4.2 Fehlerbehebung bei Updates über Update-Mirror

Je nachdem, welche Methode für den Zugriff auf den Mirror-Ordner verwendet wird, können verschiedene Probleme auftreten. Die meisten Probleme mit Updates von einem Update-Mirror haben eine oder mehrere der folgenden Ursachen: falsche Einstellungen oder Authentifizierungsdaten für den Mirror-Ordner, falsche Konfiguration auf lokalen Computern, die versuchen, Update-Dateien vom Update-Mirror herunterzuladen, oder eine Kombination der angegebenen Gründe. Hier erhalten Sie einen Überblick über die am häufigsten auftretenden Probleme bei Updates von einem Update-Mirror:

- **ESET NOD32 Antivirus meldet einen Fehler bei der Verbindung mit dem Mirror-Server** – Wahrscheinlich wird dieser Fehler durch falsche Angaben zum Update-Server (Netzwerkpfad zum Mirror-Ordner) verursacht, von dem die lokalen Computer Updates herunterladen. Um den Ordner zu überprüfen, klicken Sie unter Windows auf **Start** > **Ausführen...**, geben den Ordnernamen ein und klicken auf **OK**. Daraufhin sollte der Inhalt des Ordners angezeigt werden.
- **ESET NOD32 Antivirus verlangt einen Benutzernamen und ein Passwort** – Es wurden wahrscheinlich falsche Authentifizierungsdaten (Benutzername und Passwort) im Bereich „Update" angegeben. Benutzername und Passwort werden für den Zugriff auf den Update-Server verwendet, über den das Programm aktualisiert wird. Vergewissern Sie sich, dass die Authentifizierungsdaten korrekt und im richtigen Format eingegeben sind. Verwenden Sie das Format *Domain/Benutzername* bzw. *Arbeitsgruppe/Benutzername* und die entsprechenden Passwörter. Auch wenn „alle" auf den Mirror-Server zugreifen

können, sollten Sie bedenken, dass deshalb nicht jedem beliebigen Benutzer der Zugriff gewährt wird. „Alle“ umfasst keine nicht autorisierten Benutzer, es bedeutet, dass alle Benutzer der Domain auf den Ordner zugreifen können. Daher müssen, auch wenn „alle“ auf den Ordner zugreifen können, in den Update-Einstellungen ein Domain-Benutzername und -Passwort eingegeben werden.

- **ESET NOD32 Antivirus meldet einen Fehler bei der Verbindung mit dem Mirror-Server** – Der für den Zugriff auf die HTTP-Version des Update-Mirror angegebene Port ist blockiert.

4.2.2 So erstellen Sie Update-Tasks

Mit der Option **Update der Signaturdatenbank** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update**, und wählen Sie im Informationsfenster die entsprechende Option aus**.**

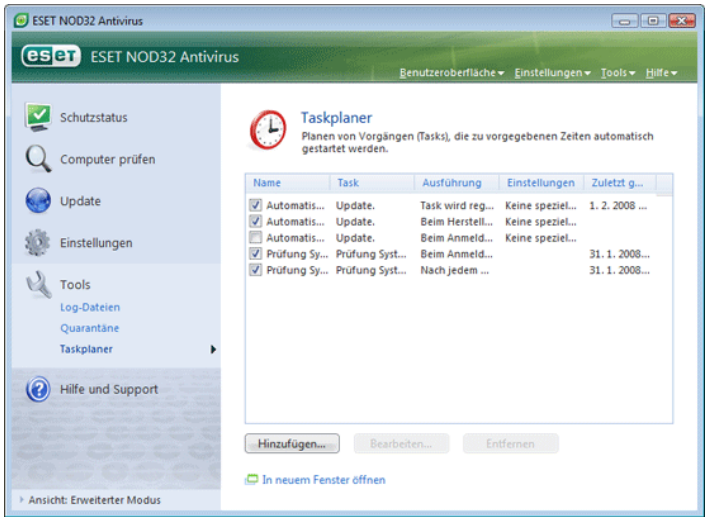
Updates können auch als geplante Vorgänge (Tasks) ausgeführt werden. Die Einstellungen für Tasks finden Sie unter **Extras > Taskplaner**. Standardmäßig sind in ESET Smart Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von -DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten- Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Kapitel „Taskplaner“.

4.3 Taskplaner

Der Taskplaner ist bei Aktivierung des erweiterten Modus von ESET NOD32 Antivirus verfügbar. Der **Taskplaner** kann im Hauptmenü von ESET NOD32 Antivirus unter **Tools** aufgerufen werden. Der Taskplaner umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive vordefiniertes Datum, Uhrzeit und verwendetes Prüfprofil.



Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates nach Herstellen von -DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Prüfung Systemstartdateien nach Anmeldung des Benutzers**
- **Prüfung Systemstartdateien nach Update der Signaturdatenbank**

Um die Konfiguration eines vorhandenen Task (sowohl standardmäßig als auch benutzerdefiniert) zu ändern, klicken Sie mit der rechten -Maustaste auf den Task und dann auf **Bearbeiten...**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten...**.

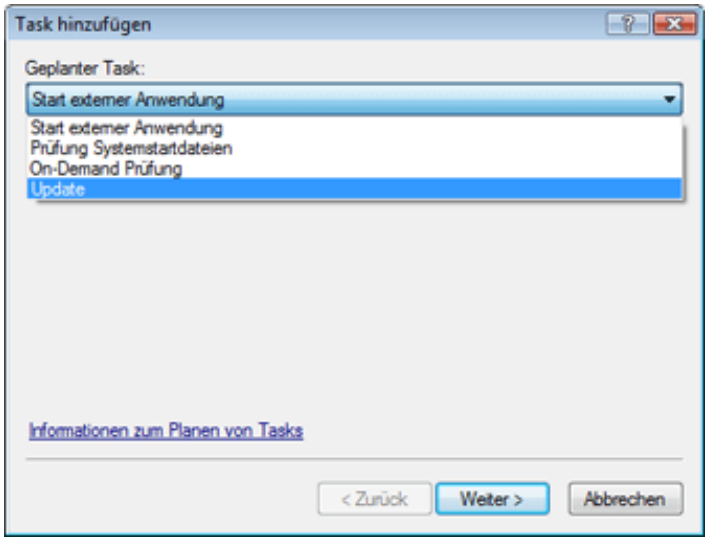
4.3.1 Verwendung von Tasks

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit sowie bestimmte Profile, die bei Ausführung des Task verwendet werden.

4.3.2 Erstellen von Tasks

Zum Erstellen eines Task im Taskplaner klicken Sie mit der rechten Maustaste auf **Hinzufügen...**, oder wählen Sie im Kontextmenü die Option **Hinzufügen...**. Es gibt fünf Arten von Tasks:

- **Start externer Anwendung**
- **Log-Wartung**
- **Prüfung Systemstartdateien**
- **Manuelles -Prüfen des Computers**
- **Update**



Da **Manuelles -Prüfen des Computers** und **Update** die meistverwendeten Tasks sind, wird hier das Hinzufügen eines neuen Update-Task beschrieben.

Wählen Sie im Dropdown-Menü **Task:** die- Option **Update**. Klicken Sie auf **Weiter**, und geben Sie den Namen des Task in das Feld **Taskname:** ein. Wählen Sie die Häufigkeit des Task. Folgende Optionen stehen zur Verfügung: **Einmalig, Wiederholt, Täglich**, **Wöchentlich** und **Bei-Ereignis**. Je nach ausgewählter Frequenz werden Ihnen verschiedene Update-Parameter angezeigt. Im nächsten Schritt können Sie eine Aktion für den Fall festlegen, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Folgende Optionen stehen zur Verfügung:

- Nächste Ausführung genau nach Planung
- Ausführung zum nächstmöglichen Zeitpunkt

- Task sofort ausführen, wenn letzte Ausführung länger zurückliegt als (die Zeit kann mit Hilfe des Felds Taskzeitraum festgelegt werden)

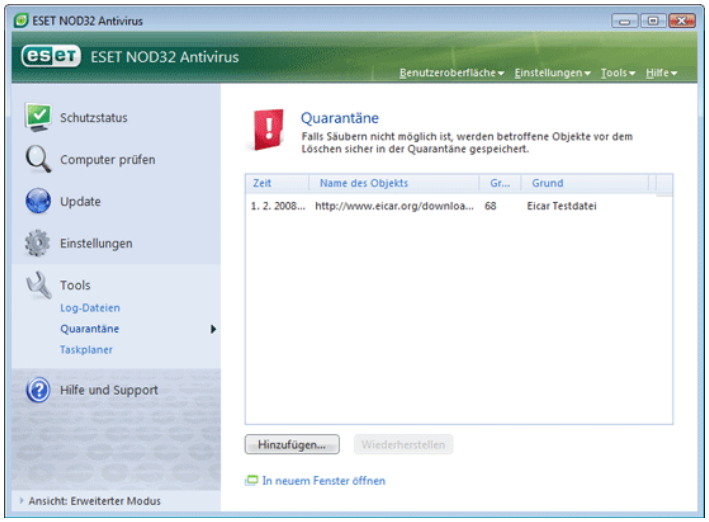
Anschließend wird eine Zusammenfassung des aktuellen Task angezeigt. Die Option „Task mit speziellen Einstellungen ausführen" sollte automatisch aktiviert sein. Klicken Sie auf „Fertig stellen".

Es wird ein Dialogfenster angezeigt, in dem Profile für den Task ausgewählt werden können. Hier können ein primäres und ein alternatives Profil festgelegt werden. Letzteres wird verwendet, falls der Task unter Verwendung des primären Profils nicht abgeschlossen werden kann. Bestätigen Sie Ihre Angaben, indem Sie im Fenster Update-Profile auf „OK" klicken. Der neue Task wird der Liste der aktuellen Tasks hinzugefügt.

4.4 Quarantäne

Die wichtigste Aufgabe der Quarantäne ist die sichere Speicherung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Smart Security fälschlicherweise erkannt worden sind.

Es können beliebige Dateien unter Quarantäne gestellt werden. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien in Quarantäne können zur Analyse an ESET gesendet werden.



Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (**Hinzugefügt durch Benutzer...**) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält.

4.4.1 Quarantäne für Dateien

Das Programm kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Hinzufügen...** klicken. In diesem Fall wird die Originaldatei nicht von ihrem ursprünglichen Speicherort entfernt. Zu diesem Zweck kann auch das Kontextmenü verwendet werden. Klicken Sie mit der rechten-Maustaste in das Quarantänefenster, und wählen Sie **Hinzufügen...**

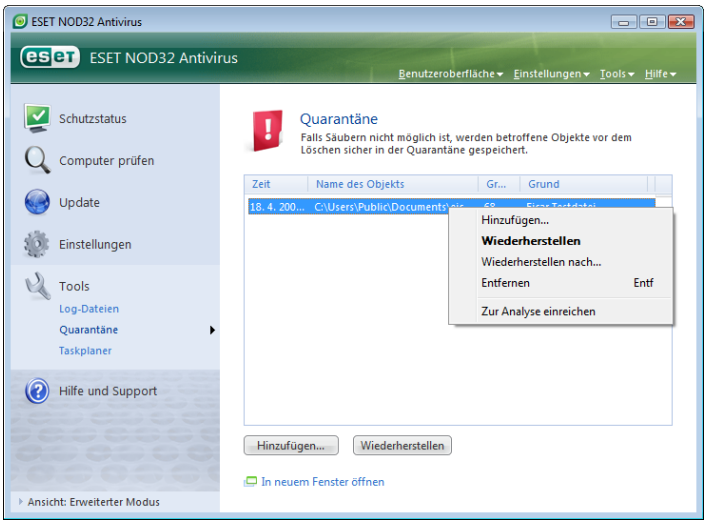
4.4.2 Wiederherstellen aus der Quarantäne

Dateien in Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie dazu die Funktion **Wiederherstellen** im Kontextmenü, das angezeigt wird, wenn Sie im Quarantänefenster mit der rechten -Maustaste auf die entsprechende Datei klicken. Das Kontextmenü enthält auch die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

HINWEIS:
Wenn versehentlich eine harmlose Datei in Quarantäne versetzt wurde, schließen Sie die Datei nach der Wiederherstellung von der Prüfung aus, und senden Sie sie an den ESET-Kundendienst.

4.4.3 Senden von Dateien in Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten- Maustaste auf die Datei, und wählen Sie im angezeigten Kontextmenü die Option **Zur Analyse senden**.



4.5 Log-Dateien

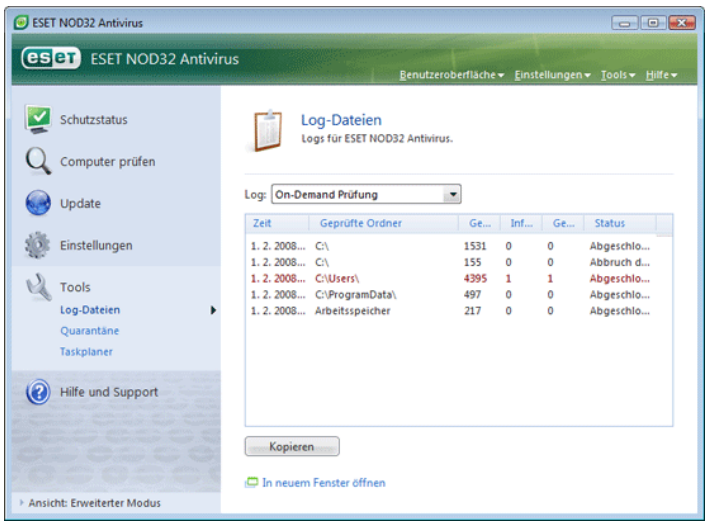
Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET NOD32 Antivirus heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

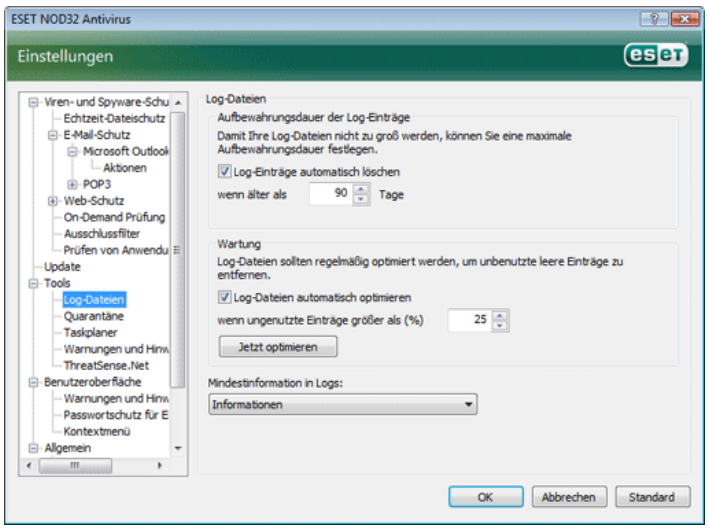
Log-Dateien können über das Hauptfenster von ESET NOD32 Antivirus aufgerufen werden, indem Sie auf **Extras > Log-Dateien** klicken. Wählen Sie oben im Fenster mit Hilfe des Dropdown-Menüs **Log:** den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen** – Über diese Option können Sie sämtliche Informationen über Ereignisse bezüglich der Erkennung eingedrungener Schadsoftware anzeigen.

2. **Ereignisse** – Diese Option kann von Systemadministratoren und Benutzern zur Lösung von Problemen verwendet werden. Alle von ESET NOD32 Antivirus ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.

3. **Manuelles- Prüfen des Computers** – In diesem Fenster werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Durch Doppelklicken- auf einen Eintrag können Sie Einzelheiten zu der entsprechenden manuellen- Prüfung anzeigen.





In jedem Abschnitt können die angezeigten Informationen direkt in die Zwischenablage kopiert werden. Dazu wählen Sie die gewünschten Einträge aus und klicken auf **Kopieren**. Um mehrere Einträge auszuwählen, können Sie die Taste STRG und die Umschalttaste verwenden.

4.5.1 Log-Wartung

Die Log-Einstellungen können über das Hauptfenster von ESET NOD32 Antivirus aufgerufen werden. Klicken Sie auf **Einstellungen > Erweiterte Einstellungen... > Tools > Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Log-Einträge automatisch löschen:** Log-Einträge, die länger als angegeben gespeichert sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren:** Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert.
- **Ausführlichkeit der Logs, mindestens:**Hier können Sie angeben, wie ausführlich die Logs sein sollen. Verfügbare Optionen:

  Kritische Fehler – Nur kritische Fehler werden protokolliert (Fehler beim Starten des Virenschutzes usw.)

  Fehler – Einfache Fehler wie „Fehler beim Herunterladen einer Datei" und kritische Fehler werden protokolliert.

  Warnungen – Kritische Fehler und Warnungen werden protokolliert.

  Hinweise – Alle Hinweise, Warnungen und Fehler werden protokolliert.

  Ereignismeldungen – Alle bisher genannten Meldungen und alle sonstigen Meldungen, die für das Beheben- von Fehlern wichtig sein können, werden protokolliert.

4.6 Benutzeroberfläche

Die Benutzeroberfläche von ESET NOD32 Antivirus lässt sich so konfigurieren, dass die Arbeitsumgebung den Bedürfnissen des Benutzers entspricht. Auf die Konfigurationsoptionen kann über die **Benutzeroberfläche** der erweiterten Einstellungen von ESET NOD32 Antivirus zugegriffen werden.

Mit den **Elementen der Benutzeroberfläche** kann der erweiterte Modus ein- und ausgeschaltet werden. Im erweiterten Modus werden erweiterte Einstellungen und zusätzliche Steuerelemente für ESET Smart Security angezeigt.

Die **Grafische Benutzeroberfläche** sollte deaktiviert werden, wenn durch die grafischen Elemente die Leistung des Computers beeinträchtigt wird oder andere Probleme auftreten. Auch bei sehbehinderten Benutzern kann die grafische Oberfläche deaktiviert werden, da Konflikte mit Spezialanwendungen zum Lesen von Text auf dem Bildschirm auftreten können.

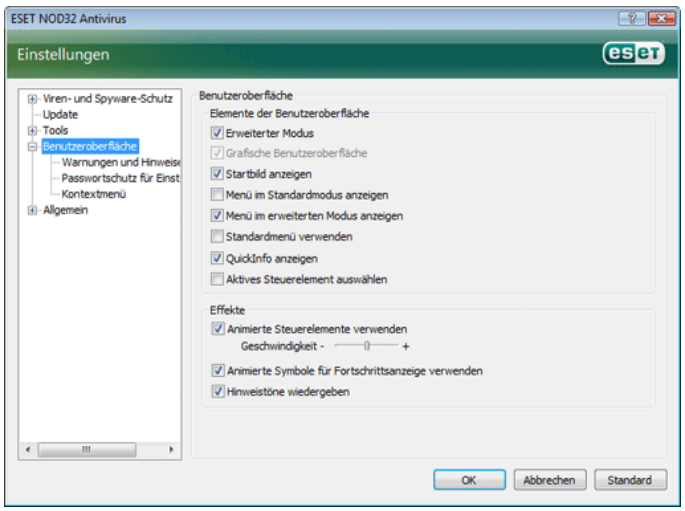
Wenn ESET NOD32 Antivirus ohne Anzeige des Startbilds- gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Oben im Hauptfenster von ESET NOD32 Antivirus befindet sich ein Standardmenü, das mit der Option **Standardmenü verwenden** aktiviert oder deaktiviert werden kann.

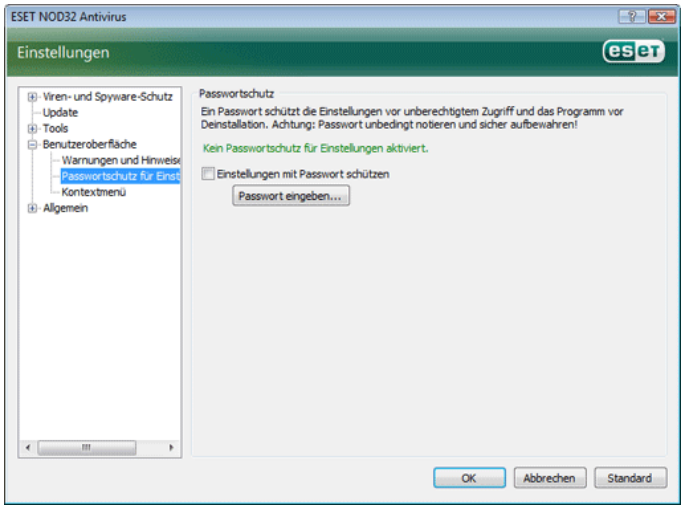
Wenn die Option **Quickinfo anzeigen** aktiviert ist, wird für jede Option, über die der Mauszeiger bewegt wird, eine kurze Beschreibung angezeigt. Mit der Option **Aktives Steuerelement auswählen** wird jedes Element hervorgehoben, das sich im aktiven Bereich des Mauszeigers befindet. Das hervorgehobene Element kann durch einen Mausklick aktiviert werden.

Um die Geschwindigkeit der animierten Effekte zu steigern oder zu reduzieren, wählen Sie die Option **Animierte Steuerelemente verwenden**, und bewegen Sie den Schieber **Geschwindigkeit** nach rechts oder links.

Um animierte Symbole zur Darstellung des Fortschritts von Aktivitäten zu verwenden, markieren Sie die Option **Animierte Symbole verwenden...**. Wenn das Programm bei wichtigen Ereignissen einen Warnton abgeben soll, markieren Sie die Option **Hinweistöne wiedergeben**.



Im Bereich **Benutzeroberfläche** befindet sich auch eine Option, um die Einstellungen von ESET NOD32 Antivirus mit einem Passwort- zu schützen. Sie wird über das Untermenü **Einstellungen schützen** der **Benutzeroberfläche** aufgerufen. Maßgeblich für einen wirksamen Schutz Ihres Systems sind die korrekten Einstellungen des Programms. Bei unzulässigen Änderungen können wichtige Daten verloren gehen. Um ein Passwort zum Schutz der Einstellungen einzurichten, klicken Sie auf **Passwort eingeben...**



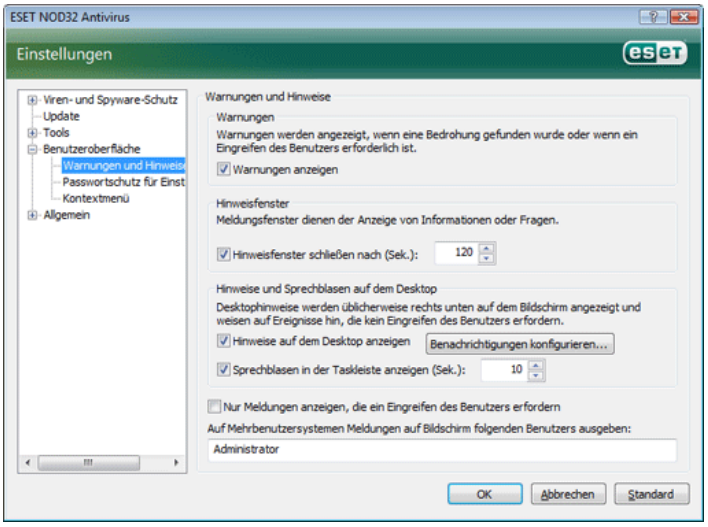
4.6.1 Warnungen und Hinweise

Unter **Benutzeroberfläche** können Sie im Bereich **Einstellungen für Warnungen und Hinweise** konfigurieren, wie Warnungen und Systemmeldungen in ESET Smart Security behandelt werden sollen.

Die erste Option ist **Warnungen anzeigen**. Bei Deaktivieren dieser Option werden keine Warnmeldungen mehr angezeigt. Diese Einstellung eignet sich nur in einigen speziellen Situationen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Wenn Popup-Fenster nach einer bestimmten Zeit automatisch geschlossen werden sollen, aktivieren Sie die Option **Hinweise automatisch schließen (Sek.)**. Die Hinweise werden nach Ablauf einer bestimmten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer manuell geschlossen worden sind.

Hinweise auf dem Desktop und Sprechblasen dienen ausschließlich zu Informationszwecken. Eingaben des Benutzers sind weder möglich noch erforderlich. Die Hinweise und Sprechblasen werden im Hinweisbereich rechts unten auf dem Bildschirm angezeigt. Zum Aktivieren der Anzeige von Desktophinweisen aktivieren Sie die Option **Hinweise auf dem Desktop anzeigen**. Weitere Optionen wie Anzeigedauer und Transparenz lassen sich einstellen, indem Sie auf **Einstellungen...** klicken. Um eine Vorschau des Verhaltens von Meldungen zu erhalten, klicken Sie auf **Vorschau**. Die Anzeigedauer von Sprechblasen lässt sich über die Option **Sprechblasen in der Taskleiste anzeigen (Sek.)** einstellen.



Im unteren Bereich des Fensters **Warnungen und Hinweise** befindet sich die Option **Nur Meldungen anzeigen, die Eingreifen des Benutzers erfordern**. Hiermit können Sie die Anzeige von Meldungen, die keine Benutzerinteraktion erfordern, aktivieren bzw. deaktivieren. Der letzte Eintrag in diesem Bereich gibt Ihnen die Möglichkeit, Adressen für Meldungen in einer Mehrbenutzerumgebung anzugeben.

Im Feld **Bei Mehrbenutzersystemen Meldungen anzeigen auf Bildschirm von Benutzer**: kann festgelegt werden, welche Personen wichtige Meldungen von ESET Smart Security erhalten. Gewöhnlich sind dies System- oder Netzwerkadministratoren. Besonders sinnvoll ist diese Option bei Terminalservern, vorausgesetzt, alle Systemmeldungen werden an den Administrator gesendet.

4.7 ThreatSense.Net

Dank des ThreatSense.Net-Frühwarnsystems erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuer Schadsoftware. Das ThreatSense.Net-Frühwarnsystem funktioniert in zwei Richtungen, hat jedoch nur einen Zweck: die Verbesserung des Schutzes, den wir Ihnen bieten. Die einfachste Möglichkeit, neue Bedrohungen zu erkennen, sobald sie in Erscheinung treten, besteht darin, so viele Kunden wie möglich zu „verknüpfen“ und als Virenscouts einzusetzen. Als Benutzer haben Sie zwei Möglichkeiten:

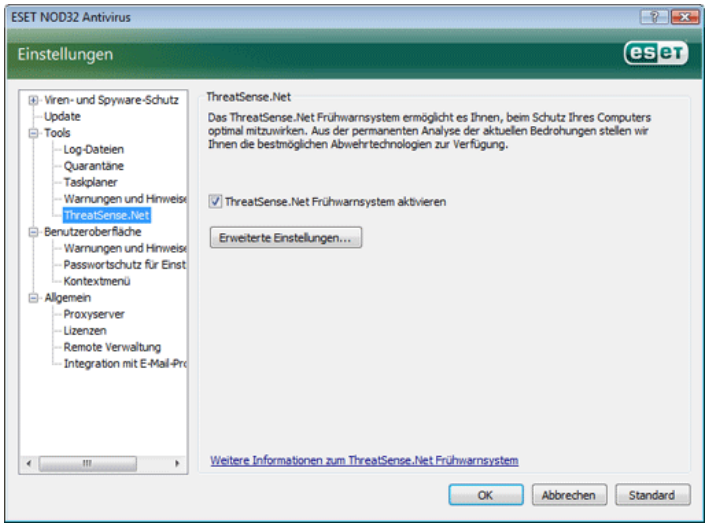
- Sie können sich entscheiden, das ThreatSense.Net-Frühwarnsystem nicht zu aktivieren. Es steht Ihnen der volle Funktionsumfang der Software zur Verfügung, und Sie erhalten auch in diesem Fall den bestmöglichen Schutz.

- Sie können das Frühwarnsystem so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym und werden in einer einzelnen Datei gesendet. Diese Datei kann zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern. Das ThreatSense.Net-Frühwarnsystem sammelt Daten über neue- Bedrohungen, die auf Ihrem Computer erkannt worden sind. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers. Bei einem Teil dieser Informationen kann es sich um persönliche Daten handeln, z. B. Benutzernamen in einem Verzeichnispfad usw. Ein Beispiel für die übermittelten Informationen ist hier verfügbar.

Auch wenn es möglich ist, dass ESET auf diese Weise gelegentlich einige Informationen über Sie oder Ihren Computer erhält, werden diese Daten für KEINEN anderen Zweck als zur Verbesserung der unmittelbaren Reaktion auf Bedrohungen verwendet.

In der Standardeinstellung von ESET NOD32 Antivirus müssen Sie das Senden verdächtiger Dateien zur genauen Analyse an ESET bestätigen. Beachten Sie, dass Dateien mit bestimmten Endungen wie .doc oder .xls stets von der Übermittlung ausgenommen sind, auch wenn eine Bedrohung darin erkannt wird. Sie können auch zusätzliche Erweiterungen hinzufügen, wenn Ihr Unternehmen vermeiden möchte, dass bestimmte Dateitypen gesendet werden.

Die Konfiguration von ThreatSense.NET kann über die erweiterten Einstellungen vorgenommen werden unter **Tools > ThreatSense.NET**. Markieren Sie das Kontrollkästchen **ThreatSense.Net-Frühwarnsystem aktivieren**. So wird die Funktion aktiviert. Klicken Sie anschließend auf **Erweiterte Einstellungen...**.

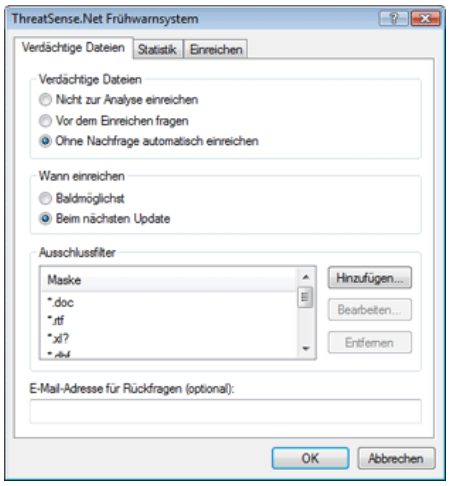


4.7.1 Verdächtige Dateien

Die Registerkarte **Verdächtige Dateien** enthält Einstellungen für das Senden von zu analysierenden Dateien an ESET.

Wenn Ihnen eine Datei verdächtig erscheint, können Sie uns diese zur Analyse senden. Sollte dabei schädlicher Code zutage treten, wird dieser beim nächsten Update der Signaturdatenbank berücksichtigt.

Die Übermittlung der Datei kann auch automatisch ohne Nachfrage erfolgen. Bei Aktivierung dieser Option werden die Dateien im Hintergrund versendet. Wenn Sie wissen möchten, welche Dateien zur Analyse gesendet werden, und Sie das Senden bestätigen möchten, wählen Sie die Option **Vor dem Senden fragen**.



Wenn keine Dateien gesendet werden sollen, wählen Sie **Nicht zur Analyse senden**. Beachten Sie, dass das Nichteinsenden von Dateien zur Analyse keine Auswirkungen auf die Übermittlung statistischer Informationen an ESET hat. Die statistischen Informationen werden in einem eigenen Bereich konfiguriert, der im folgenden Kapitel beschrieben wird.

Wann senden
Verdächtige Dateien werden so schnell wie möglich zur Analyse an ESET gesendet. Diese Einstellung wird empfohlen, wenn eine dauerhafte Internetverbindung besteht und die verdächtigen Dateien ohne Verzögerung übermittelt werden können. Die andere Option besteht darin, verdächtige Dateien **Beim nächsten Update** zu senden. In diesem Fall werden die verdächtigen Dateien gesammelt und während eines Updates auf die Server des Frühwarnsystems geladen.

Ausschlussfilter
Nicht alle Dateien müssen zur Analyse versendet werden. Über den Ausschlussfilter können Sie bestimmte Dateien oder Ordner vom Senden ausschließen. Hier können Dateien eingetragen werden, die potenziell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (Microsoft Office, OpenOffice). Die Liste der ausgeschlossenen Dateien kann beliebig erweitert werden.

E-Mail-Adresse:
Ihre E-Mail-Adresse wird zusammen mit den verdächtigen Dateien an ESET gesendet und kann dazu verwendet werden, Sie bei Fragen zu kontaktieren. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

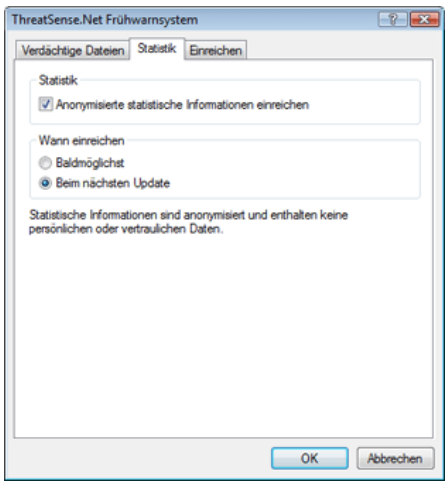
4.7.2 Statistik

Das ThreatSense.Net-Frühwarnsystem sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer von ESET NOD32 Antivirus sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Statistikpakete werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

Beispiel für ein typisches Statistikpaket:

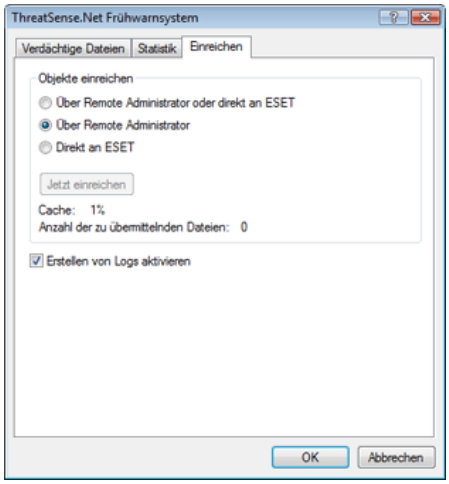
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Wann einreichen
Im Bereich **Wann senden** können Sie festlegen, wann statistische Daten gesendet werden. Wenn Sie die Option **Baldmöglichst** auswählen, werden die statistischen Daten direkt nach ihrer Erstellung gesendet. Diese Einstellung eignet sich, wenn eine dauerhafte Internetverbindung besteht. Bei der Option **Beim nächsten Update** werden die statistischen Daten gespeichert und beim nächsten Update gesammelt gesendet.



4.7.3 Senden

In diesem Bereich können Sie auswählen, ob Dateien und statistische Daten über ESET Remote Administrator oder direkt an ESET gesendet werden. Um sicherzugehen, dass verdächtige Dateien und statistische Informationen an ESET übermittelt werden, wählen Sie **Über Remote Administrator oder direkt an ESET**. Dateien und statistische Daten werden bei Auswahl dieser Option auf jeden Fall übermittelt. Beim Senden verdächtiger Dateien über Remote Administrator werden Dateien und Statistik an den Remote Administration Server gesendet, der sie an ESET weiterleitet. Bei Auswahl der Option **Direkt an ESET** werden alle verdächtigen Dateien und statistischen Daten direkt aus dem Programm an ESET gesendet.



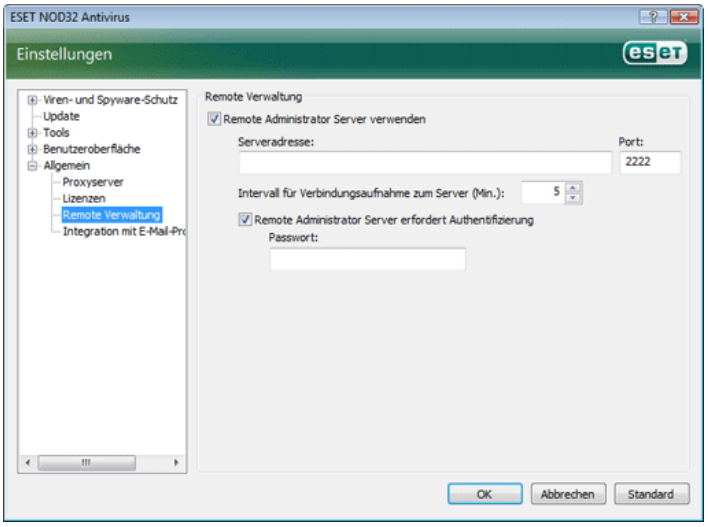
Wenn Dateien vorhanden sind, die noch gesendet werden müssen, ist die Schaltfläche **Jetzt senden** in diesem Einstellungsfenster aktiviert. Klicken Sie auf diese Schaltfläche, um die Dateien und statistischen Daten direkt zu senden.

Aktivieren Sie die Option **Erstellen von Logs aktivieren**, um Informationen über das Senden von Dateien und statistischen Daten aufzuzeichnen. Bei jeder Übertragung einer verdächtigen Datei oder statistischer Informationen wird ein Eintrag im Log erstellt.

4.8 Remoteverwaltung

Die Remoteverwaltung ist ein leistungsfähiges Tool, um Sicherheitsrichtlinien umzusetzen und einen Überblick über die Sicherheit im gesamten Netzwerk zu erhalten. Besonders sinnvoll erweist sie sich bei größeren Netzwerken. Die Remoteverwaltung bringt nicht nur ein höheres Maß an Sicherheit mit sich, sondern ermöglicht auch die benutzerfreundliche-Verwaltung von ESET NOD32 Antivirus auf Clientcomputern.

Die Optionen des Dialogfensters „Remoteverwaltung" können über das Hauptfenster von ESET NOD32 Antivirus aufgerufen werden. Klicken Sie auf **Einstellungen > Erweiterte Einstellungen... > Allgemein > Remoteverwaltung**.



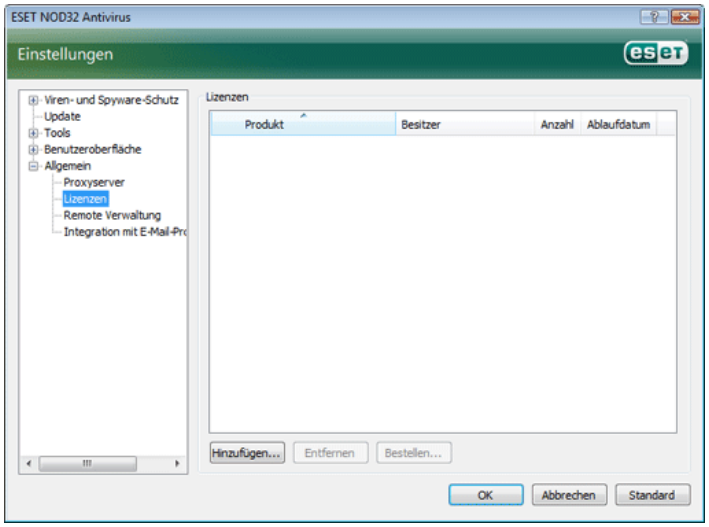
Im Fenster „Einstellungen" können Sie die Remoteverwaltung aktivieren, indem Sie das Kontrollkästchen **Remote Administrator Server verwenden** aktivieren. Anschließend können Sie auf folgende Optionen zugreifen:

- **Serveradresse** – Netzwerkadresse des Servers, auf dem der Remoteverwaltungsserver installiert ist.
- **Port** – Dieses Feld enthält einen vordefinierten Port für die Verbindung mit dem Server. Es wird empfohlen, den voreingestellten Port 2222 zu verwenden.
- **Intervall für Verbindungsaufnahme zum Server (Min.)** – Hier wird die Häufigkeit angegeben, mit der ESET NOD32 Antivirus eine Verbindung zum ERA-Server herstellt, um Daten zu übertragen. Mit anderen Worten, die Daten werden in den hier festgelegten Zeitabständen gesendet. Bei der Einstellung 0 werden alle 5 Sekunden Daten gesendet.
- **Remote Administrator Server erfordert Authentifizierung** – Falls erforderlich, können Sie hier ein Passwort für die Verbindung zum Remoteverwaltungsserver eingeben.

Klicken Sie auf **OK,** um die geänderten Einstellungen zu übernehmen. ESET NOD32 Antivirus nutzt diese Einstellungen zur Verbindung mit dem Remoteserver.

4.9 Lizenz

Unter **Lizenz** werden die Lizenzschlüssel für ESET NOD32 Antivirus und andere ESET-Produkte verwaltet. Nach dem Erwerb erhalten Sie die Lizenzschlüssel zusammen mit Ihrem Benutzernamen und dem Passwort. Klicken Sie auf die Schaltflächen **Hinzufügen/Entfernen**, um Lizenzen hinzuzufügen bzw. zu entfernen. Der Lizenzmanager befindet sich in den erweiterten Einstellungen unter **Allgemein > Lizenzen.**



Beim Lizenzschlüssel handelt es sich um eine Textdatei mit Informationen zum erworbenen Produkt: Eigentümer, Anzahl der Lizenzen und Ablaufdatum.

Im Fenster „Lizenzmanager" kann der Inhalt eines Lizenzschlüssels geladen und angezeigt werden. Durch Klicken auf **Hinzufügen...** werden die in der Datei enthaltenen Informationen im Lizenzmanager angezeigt. Um Lizenzdateien aus der Liste zu löschen, wählen Sie **Entfernen**.

Wenn ein Lizenzschlüssel abgelaufen ist und Sie die Lizenz erneuern möchten, klicken Sie auf **Bestellen...** – Sie werden zu unserem Online-Shop weitergeleitet.

5. Erfahrene Benutzer

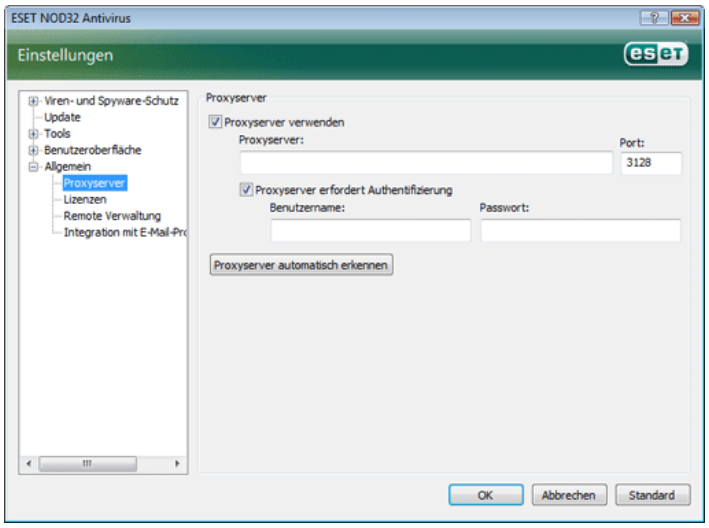
In diesem Kapitel werden Funktionen von ESET NOD32 Antivirus beschrieben, die besonders für erfahrene Benutzer geeignet sind. Die entsprechenden Optionen stehen ausschließlich im erweiterten Modus zur Verfügung. Um in den erweiterten Modus zu wechseln, klicken Sie im Hauptfenster des Programms links unten auf **Erweiterter Modus Ein/Aus**, oder drücken Sie STRG + M.

5.1 Einstellungen für den Proxyserver

Bei ESET Smart Security kann die Konfiguration des Proxyservers in zwei unterschiedlichen Bereichen der erweiterten Einstellungen vorgenommen werden.

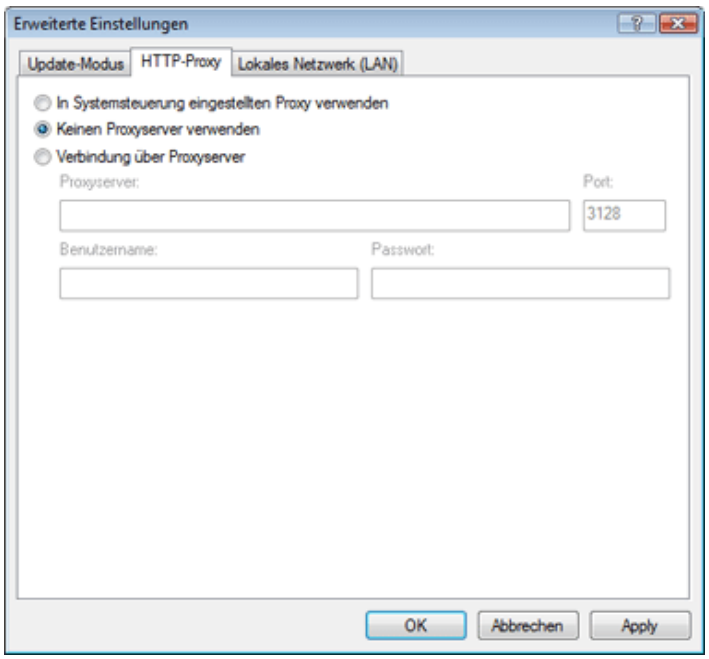
Zum einen können Sie die Einstellungen des Proxyservers unter **Allgemein > Proxyserver** konfigurieren. Dadurch werden die allgemeinen Einstellungen des Proxyservers für ganz ESET Smart Security übernommen. Die Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

Um die Einstellungen des Proxyservers für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Folgenden Proxyserver verwenden**, und geben Sie im Feld **Proxyserver:** die entsprechende Adresse zusammen mit der **Port**nummer des Proxyservers ein.



Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxyserver erfordert Authentifizierung**, und geben Sie einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf die Schaltfläche **Proxyserver automatisch erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Dann werden die Parameter aus dem Internet Explorer kopiert. Beachten Sie, dass mit Hilfe dieser Funktion keine Authentifizierungsdaten (Benutzername und Passwort) abgerufen werden. Diese müssen vom Benutzer selbst eingegeben werden.

Die Konfiguration des Proxyservers kann aber auch in den **Erweiterten Einstellungen Update** (Option **Update** der erweiterten Einstellungen) vorgenommen werden. Diese Einstellungen gelten für das aktuelle Update-Profil und werden für Laptops empfohlen, da diese die Updates der Virensignaturen häufig von verschiedenen Standorten beziehen. Mehr Informationen zu diesen Einstellungen erhalten Sie im Abschnitt 4.4 „Aktualisierung des Systems".



5.2 Einstellungen exportieren/importieren

Die aktuelle Konfiguration von ESET NOD32 Antivirus kann im erweiterten Modus unter **Einstellungen**exportiert bzw. importiert werden.

Für Im- und Exporte wird der Dateityp .xml verwendet. Importe und Exporte sind dann hilfreich, wenn Sie die aktuelle Konfiguration von ESET NOD32 Antivirus zur späteren Verwendung sichern möchten (aus unterschiedlichen Gründen). Die Funktion zum Export der Einstellungen werden vor allem jene zu schätzen wissen, die ihre bevorzugte Konfiguration von ESET NOD32 Antivirus auf verschiedene Computer übertragen möchten: Sie müssen lediglich die entsprechende .xml-Datei importieren.

5.2.1 Einstellungen exportieren

Die Konfiguration lässt sich problemlos exportieren. Wenn Sie die aktuellen Einstellungen von ESET Smart Security speichern möchten, klicken Sie auf **Einstellungen > Einstellungen importieren und exportieren...**. Markieren Sie die Option **Einstellungen exportieren**, und geben Sie den Namen der Konfigurationsdatei ein. Suchen Sie mit Hilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

5.2.2 Einstellungen importieren

Der Import von Einstellungen verläuft sehr ähnlich. Wählen Sie erneut **Einstellungen importieren und exportieren**, und markieren Sie die Option **Einstellungen importieren**. Klicken Sie auf die Schaltfläche**...**, und suchen Sie nach der Konfigurationsdatei, die Sie importieren möchten.

5.3 Kommandozeile

Das Virenschutz-Modul von ESET NOD32 Antivirus kann über die Kommandozeile gestartet werden, entweder manuell (mit dem Befehl „ecls") oder über eine Batch-Datei („.bat").

Folgende Parameter und Switches stehen zur Verfügung, um die manuelle Prüfung über die Kommandozeile auszuführen: -Allgemeine Befehle:

Allgemeine Befehle:

– help	Hilfe anzeigen und verlassen
– version	Versionsinformationen anzeigen und verlassen
– base-dir = FOLDER	Module aus dem Ordner FOLDER laden
– quar-dir = FOLDER	Quarantäneordner (FOLDER) angeben
– aind	Aktivitätsanzeige anzeigen
-- auto	Alle Festplatten im Entfernungsmodus prüfen

Zu prüfende Objekte:

– files	Dateien prüfen (Standardeinstellung)
– no-files	Dateien nicht prüfen
– boots	Bootsektoren prüfen (Standardeinstellung)
– no-boots	Bootsektoren nicht prüfen
– arch	Archive prüfen (Standardeinstellung)
– no-arch	Archive nicht prüfen
– max-archive-level = LEVEL	Maximale Verschachtelungsstufe (LEVEL) bei Archiven
– scan-timeout = LIMIT prüfen. Wenn die die Prüfung des	Archive maximal für LIMIT (Sekunden) angegebene Zeit abgelaufen ist, wird Archivs beendet und bei der nächsten Datei fortgesetzt.
– max-arch-size=SIZE	Nur die ersten SIZE Byte in Archiven prüfen (Standardeinstellung: 0 = unbegrenzt)
– mail	E-Mail-Dateien prüfen
– nomail	E-Mail-Dateien nicht prüfen
– sfx	Selbstentpackende Archive prüfen
– nosfx	Selbstentpackende Archive nicht prüfen
– rtp	Laufzeitkomprimierte Dateien prüfen
– nortp	Laufzeitkomprimierte Dateien nicht prüfen
– exclude = FOLDER	Ordner FOLDER von der Prüfung ausschließen
– subdir	Untergeordnete Verzeichnisse prüfen (Standardeinstellung)
– nosubdir	Untergeordnete Verzeichnisse nicht prüfen
– maxsubdirlevel = LEVEL	Maximale Verschachtelungsstufe (LEVEL) bei untergeordneten Verzeichnissen (Standardeinstellung: 0 = unbegrenzt)
– symlink	Symbolischen Verknüpfungen folgen (Standardeinstellung)
– nosymlink	Symbolische Verknüpfungen übergehen
– extremove = EXTENSIONS	
– extexclude = EXTENSIONS	Durch einen Doppelpunkt getrennte Erweiterungen (EXTENSIONS) von der Prüfung ausschließen

Methoden:

– adware	Auf Adware/Spyware/Riskware prüfen
– no-adware	Nicht auf Adware/Spyware/Riskware prüfen
– unsafe	Auf potenziell unsichere Anwendungen prüfen
– no-unsafe	Nicht auf potenziell unsichere Anwendungen prüfen
– unwanted	Auf potenziell unerwünschte Anwendungen prüfen
– no-unwanted	Nicht auf potenziell unerwünschte Anwendungen prüfen
– pattern	Signaturen verwenden
– no-pattern	Signaturen nicht verwenden
– heur	Heuristik aktivieren
– no-heur	Heuristik deaktivieren
– adv-heur	Advanced Heuristik aktivieren
– no-adv-heur	Erweiterte Heuristik deaktivieren

Schadcode entfernen:

– action = ACTION	Aktion ACTION für infizierte Objekte ausführen Mögliche Aktionen: none, clean, prompt (keine, Schadcode entfernen, Aufforderung anzeigen)
– Quarantäne	Infizierte Dateien in Quarantäneordner kopieren (ergänzt ACTION)
– noquarantine	Infizierte Dateien nicht in Quarantäneordner kopieren**Logs:**
– log-file=FILE	Ausgabe in Datei FILE aufzeichnen
– log-rewrite	Ausgabedatei überschreiben (Standardeinstellung: append (anhängen)
– logall	Nicht infizierte Dateien ebenfalls ins Log aufnehmen
– nologall	Nicht infizierte Dateien nicht ins Log aufnehmen (Standardeinstellung) Mögliche Exit-Codes der Prüfung:

0 – Keine Bedrohung gefunden
1 – Bedrohung gefunden, aber nicht entfernt
10 – Noch mehrere infizierte Dateien vorhanden
101 – Archivierungsfehler
102 – Zugriffsfehler
103 – interner Fehler

HINWEIS:

Exit-Codes über 100 bedeuten, dass die Datei nicht geprüft wurde und daher infiziert sein kann.

6. Glossar

6.1 Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die in einen Computer eindringt und/oder auf einem Computer Schaden anrichtet.

6.1.1 Viren

Bei einem Computervirus handelt es sich um eingedrungene Schadsoftware, die auf Ihrem Computer befindliche Dateien beschädigt. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich vom einen zum anderen Computer auszubreiten.

Computerviren greifen hauptsächlich ausführbare Dateien und Dokumente an. Um sich zu vermehren, hängt sich ein Virus mit seinem „Körper" an das Ende einer Zieldatei an. Und so funktioniert ein Computervirus: Durch Ausführung der infizierten Datei wird der Virus aktiviert (noch bevor die eigentliche Anwendung gestartet wird) und führt seine vordefinierte Task aus. Erst dann wird die eigentliche Anwendung gestartet. Ein Virus kann einen Computer also nur dann infizieren, wenn der Benutzer selbst (versehentlich oder absichtlich) das bösartige Programm ausführt oder öffnet.

Computerviren unterscheiden sich durch Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen wirklichen Schaden verursachen – ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Es soll an dieser Stelle jedoch darauf hingewiesen werden, dass Viren (verglichen mit Trojanern oder Spyware) allmählich immer mehr zur Seltenheit werden, da sie für Urheber von bösartiger Software aus kommerzieller Sicht nicht attraktiv sind. Außerdem wird der Begriff „Virus" oft fälschlicherweise für alle Arten von Schadsoftware verwendet. obwohl sich gegenwärtig nach und nach der neue, zutreffendere Begriff „Malware" (bösartige Software) durchsetzt.

Wenn Ihr Computer von einem Virus infiziert wurde, ist es notwendig, den Originalzustand der infizierten Dateien wiederherzustellen – das heißt, den Schadcode mit Hilfe eines Virenschutzprogrammes daraus zu entfernen.

Beispiele für Viren sind: OneHalf, Tenga und Yankee Doodle.

6.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das einen bösartigen Code enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Das heißt, sie sind unabhängig von Wirtsdateien (oder Bootsektoren).

Würmer verbreiten sich entweder über E-Mails oder über Netzwerkpakete. Diesbezüglich werden zwei Arten unterschieden:

- **E-Mail-Würmer** – Würmer, die sich selbstständig über E-Mail-Adressen aus der Kontaktliste eines Nutzers verbreiten.
- **Netzwerkwürmer** – Würmer, die die Sicherheitslücken verschiedener Anwendungen ausnutzen.

Würmer sind daher wesentlich flexibler als Viren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden über den gesamten Globus verbreiten – in manchen Fällen gelingt ihnen dies sogar schon in wenigen Minuten. Wegen dieser Fähigkeit, sich unabhängig und rasant zu vermehren, sind Würmer denn auch gefährlicher als andere Arten von Malware, wie z. B. Viren.

Ein in einem System aktiver Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder gar Programme deaktivieren.

Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Angriffen fungieren.

Wenn Ihr Computer mit einem Wurm infiziert ist, empfehlen wir Ihnen, die infizierten Dateien zu löschen, da sie wahrscheinlich bösartigen Code enthalten.

Beispiele für bekannte -Würmer sind: Lovsan/Blaster, Stration/Warezov, Bagle und Netsky.

6.1.3 Trojaner

Trojaner galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten. Dies gilt jedoch nur für die erste Trojaner-Generation. Inzwischen müssen sich Trojaner nicht mehr tarnen. Ihr einzige Absicht besteht darin, sich möglichst leicht Zugang zu einem System zu verschaffen, um dort den gewünschten Schaden anzurichten. Der Begriff „Trojaner" ist zu einem sehr allgemeinen Begriff geworden, der jegliche Form von Schadsoftware beschreibt, die nicht einer bestimmten Kategorie zugeordnet werden kann.

Aus diesem Grund wird die Kategorie „Trojaner" oft in mehrere Gruppen unterteilt. Die bekanntesten davon sind:

- Downloader – ein bösartiges Programm zum Herunterladen von Schadsoftware aus dem Internet.
- Dropper – Trojaner, der auf angegriffenen Computern weitere Malware absetzt.
- Backdoor – Anwendung, die externen Angreifern Zugang zu einem System verschafft, um es zu übernehmen.
- Keylogger – Programm, das die Tastenanschläge von Benutzern aufzeichnet und die gewonnenen Daten an den Angreifer sendet.
- Dialer – Programme, die Wählverbindungen zu teuren-Einwahlnummern herstellen. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von -Einwahlmodems. Darum werden Dialer auch nur noch selten eingesetzt.

Trojaner sind in der Regel ausführbare Dateien mit der Erweiterung „.exe". Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Zu den -bekanntesten Trojanern zählen: NetBus, Trojandownloader. Small.ZL, Slapper

6.1.4 Rootkits

Rootkits sind bösartige Programme, die Hackern unbegrenzten und verdeckten Zugriff auf ein System verschaffen. Nach dem Zugriff auf ein System (in der Regel unter Ausnutzung einer Sicherheitslücke) greifen Rootkits auf Funktionen des Betriebssystems zurück, um nicht von der Virenschutz-Software erkannt zu werden: Prozesse, Dateien und Windows-Registrierungsdaten werden versteckt. Aus diesem Grund ist es nahezu unmöglich, Rootkits mithilfe der üblichen Prüfmethoden zu erkennen.

Bei der Rootkit-Prävention müssen Sie beachten, dass Rootkits auf zwei verschiedenen Ebenen erkannt werden können:

1. Beim Zugriff auf ein System. Die Rootkits haben das System noch nicht befallen, sind also inaktiv. Die meisten Virenschutzsysteme können Rootkits auf dieser Ebene entfernen (vorausgesetzt, dass solche Dateien auch als infizierte Dateien erkannt werden).
2. Wenn sich die Rootkits vor den regulären Prüfmethoden verstecken. Benutzer des ESET-Virenschutzsystems haben den Vorteil der Anti--Stealth-Technologie, die auch aktive Rootkits erkennen und entfernen kann.

6.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising)-unterstützte Software. In diese Kategorie fallen Programme, die zur Anzeige von Werbung dienen. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, da die Freeware-Entwickler damit die Entwicklungskosten ihrer (in der Regel nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich, doch werden Benutzer mit Werbung belästigt. Bedenklich ist Adware, da sie auch dazu dienen kann, Daten zu sammeln (genauso wie Spyware).

Wenn Sie sich für die Verwendung eines Freeware-Produkts entscheiden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren. In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware oder nur mit eingeschränktem Funktionsumfang installieren. Das bedeutet, dass Adware häufig ganz „legal" auf das System zugreift, da sich die Benutzer damit einverstanden erklärt haben. In diesem Fall gilt: Vorsicht ist besser als Nachsicht.

Wenn auf Ihrem Computer eine Datei als Adware erkannt wird, sollten Sie sie löschen, da sie in den meisten Fällen bösartigen Code umfasst.

6.1.6 Spyware

Der Begriff „Spyware" fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. Listen der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Autoren von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, -gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten können Sicherheitscodes, PINs, Kontonummern usw. umfassen. Spyware wird oft im Paket mit der kostenlosen Version eines Programms zum Download angeboten, um Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie dadurch zu einem Upgrade auf die kommerzielle Version ohne Spyware zu bewegen.

Beispiele für bekannte-Freeware-Produkte, die zusammen mit Spyware heruntergeladen werden, sind Client-Anwendungen für P2P-Netzwerke (Peer--to--Peer). Programme wie Spyfalcon oder Spy Sheriff gehören zu einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.7 Potenziell unsichere Anwendungen

Es gibt zahlreiche rechtmäßige Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie allerdings missbraucht werden, können Sie durchaus schädliche Wirkung haben. Darum wurde von ESET diese spezielle Kategorie geschaffen. Unsere Kunden haben nun die Option zu wählen, ob solche Bedrohungen vom Virenschutzsystem erkannt werden sollen oder nicht.

Zur Kategorie der „potenziell unsicheren Anwendungen" zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu gehören Programme für das Fernsteuern von Computern (per Fernzugriff), Programme zum Entschlüsseln von Passwörtern- und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen Sie die Anwendung.

6.1.8 Potenziell unerwünschte Anwendungen

Bei potenziell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Die gravierendsten Veränderungen sind:

- neue Fenster werden angezeigt
- versteckte Prozesse werden gestartet
- Prozessor und Speicher werden stärker belastet als zuvor
- Suchergebnisse ändern sich
- die Anwendung kommuniziert mit Servern im Internet